MATHEMATICS OF COMPUTATION
Volume 88, Number 317, May 2019, Pages 1341–1390
https://doi.org/10.1090/mcom/3370
Article electronically published on August 1, 2018

COMPUTING ELLIPTIC CURVES OVER $\mathbb{Q}$

MICHAEL A. BENNETT, ADELA GHERGA, AND ANDREW RECHNITZER

Abstract. We discuss an algorithm for finding all elliptic curves over $\mathbb{Q}$ with a given conductor. Though based on classical ideas derived from reducing the problem to one of solving associated Thue-Mahler equations, our approach, in many cases at least, appears to be reasonably efficient computationally. We provide details of the output derived from running the algorithm, concentrating on the cases of conductor p or p^2, for p prime, with comparisons to existing data.

1. Introduction

A classical result of Shafarevich [58] implies that, given a fixed set of prime numbers S, there are only finitely many $\mathbb{Q}$-isomorphism classes of elliptic curves defined over $\mathbb{Q}$ with good reduction outside S. In 1970, Coates [13] proved an effective version of this theorem, using bounds for linear forms in p-adic and complex logarithms. Early attempts to make these results explicit, for fixed sets of small primes, overlap with the arguments of [13], in that they reduce the problem to solving a number of *Thue-Mahler equations*. These are Diophantine equations of the form

$$F(x, y) = u. \tag{1}$$

Here, F is a binary form of degree 3 or greater, with integer coefficients, and u is an S-*unit*—an integer whose prime factors are contained in S. The number of solutions in relatively prime integers x and y to equation (1), provided that F is irreducible, is known to be finite, via the work of Mahler [39]. This generalizes a classical result of Thue [66] who had proved an analogous statement for the case of u fixed in equation (1). When F is a reducible form in $\mathbb{Z}[x, y]$, equation (1) is typically less difficult to solve; in the context of finding elliptic curves, this situation arises from consideration of elliptic curves with at least one nontrivial rational 2-torsion point. The first examples where all elliptic curves $E/\mathbb{Q}$ with good reduction outside a given set S were determined for $S = \{2, 3\}$ by Coghlan [14] and Stephens [64] (see also [8]), and for $S = \{p\}$ for certain small primes p; see, e.g., Setzer [57] and Neumann [48]. Each of these examples corresponds, via our approach, to cases with reducible forms. Agrawal, Coates, Hunt, and van der Poorten [1] carried out the first analysis where irreducible forms in equation (1) were treated to find elliptic curves of given conductor (dealing with the case $S = \{11\}$). In this situation, the reduction to equation (1) is not particularly involved, but subsequent computations

Received by the editor October 6, 2017, and, in revised form, November 1, 2017, February 21, 2018, and March 16, 2018.
2010 *Mathematics Subject Classification.* Primary 11D45, 11D61; Secondary 11J82, 11J86.
The authors were supported in part by NSERC.

are quite difficult; they use arguments from [13] and a range of techniques from computational Diophantine approximation.

It appears that there are very few subsequent attempts in the literature to compute elliptic curves of a given conductor through the solution of Thue-Mahler equations. Instead, one finds a wealth of results which approach the problem via modular forms. This route relies upon the Modularity theorem (see Wiles [73] and Breuil, Conrad, Diamond, and Taylor [10]), which was actually still conjectural when these ideas were first implemented. To find all $E/\mathbb{Q}$ of conductor N by this method, one computes the space of $\Gamma_0(N)$ modular symbols and the action of the Hecke algebra on it, and then searches for one-dimensional rational eigenspaces. After calculating a large number of Hecke eigenvalues, one is then able to extract corresponding elliptic curves. For a detailed description of how this technique works, the reader is directed to [16]. The great computational success of this approach can be primarily attributed to Cremona (see, e.g., [15], [16]) and his collaborators; they have devoted many years of work to it and are responsible for the current state-of-the-art. In particular, at the time of writing in 2017, all $E/\mathbb{Q}$ of conductor $N \leq 400000$ have been determined by these methods.

In the paper at hand, we return to techniques based upon solving Thue-Mahler equations, using a number of results from classical invariant theory. Our aim is to give a straightforward demonstration of the link between the conductors in question and the corresponding equations, and to make the Diophantine approximation problem that follows as easy to tackle as possible. It is worth noting here that these connections are quite straightforward for primes $p > 3$, but require careful analysis at the primes 2 and 3. We will demonstrate our approach for a number of specific conductors and sets S, and then focus our main computational efforts on curves with bad reduction at a single prime (i.e., curves of conductor p or p^2 for p prime). In these cases, the computations simplify significantly and we are able to find all curves of prime conductor up to 2×10^9 (10^{10} in the case of curves of positive discriminant) and conductor p^2 for $p \leq 5 \times 10^5$. We then extend these computations in the case of conductor p, for prime $p \leq 2 \times 10^{13}$, and conductor p^2 for prime $p \leq 10^{10}$. We are not, however, able to guarantee completeness for these extended computations (we will discuss this further in what follows).

The outline of this paper is as follows. In Section 2, we discuss some basic facts about elliptic curves, with corresponding notation. In Section 3, we review the invariant theory of cubic forms and state our main theorem upon which our algorithm is based. Section 4 contains the proof of this theorem. Section 5 is devoted to the actual computation of the cubic forms we require. We provide a few examples of our approach for composite conductors in Section 6. Specifically, we find all elliptic curves $E/\mathbb{Q}$ with conductor N for

$$N \in \{399993, 999999, 999999999, 2655632887, 3305354359\}$$

and all $E/\mathbb{Q}$ with good reduction outside S, where

$$S = \{2, 3, 23\} \quad \text{and} \quad S = \{2, 3, 5, 7, 11\}.$$

These last two examples have been considered recently by other authors ([36] and [37]), using different techniques.

The remainder of the paper is devoted to finding curves with bad reduction at a single prime p, i.e., those of conductor $N = p$ or p^2. We indicate in Section 7 how the problem of computing elliptic curves over $\mathbb{Q}$ of fixed conductor simplifies

considerably in such a situation and set the stage for our main computation. In Section 8, we provide a variety of further details for these cases and an outline of a heuristic approach to the problem that enables us to work with curves of quite large conductor (allowing us to find, in all likelihood, all elliptic curves of prime conductor p for $p < 2\times 10^{13}$). Here, the obstruction to a deterministic solution to our problem for such large values of p is provided by the existence of extremely large fundamental units in corresponding cubic fields. Section 9 contains an overview of our output, with comparisons to previous results in the literature. Finally, in Section 10, we provide an argument to show that any elliptic curve that has not been detected by our "heuristic" approach corresponds to a record-setting "Hall ratio", that is, an example of integers x and y where the (nonzero) difference $|x^3 - y^2|$ is unusually small.

2. Elliptic curves

Our basic problem is to find a model for each isomorphism class of elliptic curves over $\mathbb{Q}$ with a given conductor. Let $S = \{p_1, p_2, \ldots, p_k\}$, where the p_i are distinct primes, and fix a conductor $N = p_1^{\eta_1} \cdots p_k^{\eta_k}$ for $\eta_i \in \mathbb{N}$. Any curve of conductor N has a minimal model

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with the a_i integral and discriminant

$$\Delta_E = (-1)^\delta p_1^{\gamma_1} \cdots p_k^{\gamma_k},$$

where the γ_i are positive integers satisfying $\gamma_i \geq \eta_i$, for each $i = 1, 2, \ldots, k$, and $\delta \in \{0, 1\}$.

Writing

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6, \quad c_4 = b_2^2 - 24b_4$$

and

$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$$

we have $1728\Delta_E = c_4^3 - c_6^2$ and $j_E = c_4^3/\Delta_E$. It follows that

$$c_6^2 = c_4^3 + (-1)^{\delta+1} 2^6 \cdot 3^3 \cdot p_1^{\gamma_1} \cdots p_k^{\gamma_k}. \tag{2}$$

In fact, it is equation (2) that lies at the heart of our method (see also Cremona and Lingham [19] for an approach to the problem that takes as its starting point equation (2), but subsequently heads in a rather different direction).

Let $\nu_p(x)$ be the largest power of a prime p dividing a nonzero integer x. Since our model is minimal, we may suppose (via Tate's algorithm; see, for example, Papadopoulos [49]) that

$$\min\{3\nu_p(c_4), 2\nu_p(c_6)\} < 12 + 12\nu_p(2) + 6\nu_p(3),$$

for each prime p, while

$$\nu_p(N_E) \leq 2 + \nu_p(1728).$$

For future use, it will be helpful to have a somewhat more precise determination of the possible values of $\nu_p(c_4)$ and $\nu_p(c_6)$ we encounter. We compile this data from Papadopoulos [49] and summarize it in Tables 1, 2, and 3.

TABLE 1. The possible values of $\nu_2(c_4), \nu_2(c_6), \nu_2(\Delta_E)$ and $\nu_2(N)$.

$\nu_2(c_4)$	$\nu_2(c_6)$	$\nu_2(\Delta_E)$	$\nu_2(N)$
0	0	≥ 0	$\min\{1, \nu_2(\Delta_E)\}$
≥ 4	3	0	0
≥ 4	5	4	2, 3 or 4
≥ 4	≥ 6	6	5 or 6
4	6	7	7
4	6	8	2, 3 or 4
4	6	9	5
4	6	10 or 11	3 or 4
4	6	≥ 12	4
5	7	8	7
≥ 6	7	8	2, 3 or 4

$\nu_2(c_4)$	$\nu_2(c_6)$	$\nu_2(\Delta_E)$	$\nu_2(N)$
5	≥ 8	9	8
≥ 6	8	10	6
6	≥ 9	12	5 or 6
6	9	≥ 14	6
7	9	12	5
≥ 8	9	12	4
6	9	13	7
7	10	14	7
7	≥ 11	15	8
≥ 8	10	14	6

TABLE 2. The possible values of $\nu_3(c_4), \nu_3(c_6), \nu_3(\Delta_E)$ and $\nu_3(N)$.

$\nu_3(c_4)$	$\nu_3(c_6)$	$\nu_3(\Delta_E)$	$\nu_3(N)$
0	0	≥ 0	$\min\{1, \nu_3(\Delta_E)\}$
1	≥ 3	0	0
≥ 2	3	3	2 or 3
2	4	3	3
2	≥ 5	3	2
2	3	4	4
2	3	5	3
2	3	≥ 6	2
≥ 3	4	5	5
3	5	6	4

$\nu_3(c_4)$	$\nu_3(c_6)$	$\nu_3(\Delta_E)$	$\nu_3(N)$
3	≥ 6	6	2
≥ 4	5	7	5
≥ 4	6	9	2 or 3
4	7	9	3
4	≥ 8	9	2
4	6	10	4
4	6	11	3
≥ 5	7	11	5
5	8	12	4
≥ 6	8	13	5

TABLE 3. The possible values of $\nu_p(c_4), \nu_p(c_6), \nu_p(\Delta_E)$ and $\nu_p(N)$ when $p > 3$ is prime and $p \mid \Delta_E$.

$\nu_p(c_4)$	$\nu_p(c_6)$	$\nu_p(\Delta_E)$	$\nu_p(N)$
0	0	≥ 1	1
≥ 1	1	2	2
1	≥ 2	3	2
≥ 2	2	4	2
≥ 2	≥ 3	6	2

$\nu_p(c_4)$	$\nu_p(c_6)$	$\nu_p(\Delta_E)$	$\nu_p(N)$
2	3	≥ 7	2
≥ 3	4	8	2
3	≥ 5	9	2
≥ 4	5	10	2

3. CUBIC FORMS: THE MAIN THEOREM AND ALGORITHM

Having introduced the notation we require for elliptic curves, we now turn our attention to cubic forms and our main result. Fix integers a, b, c, and d, and consider

the binary cubic form

$$F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3, \tag{3}$$

with discriminant

$$D_F = -27a^2d^2 + b^2c^2 + 18abcd - 4ac^3 - 4b^3d. \tag{4}$$

To any such form, we can associate a pair of covariants, the Hessian $H = H_F$:

$$H = H_F(x,y) = -\frac{1}{4}\left(\frac{\partial^2 F}{\partial x^2}\frac{\partial^2 F}{\partial y^2} - \left(\frac{\partial^2 F}{\partial x \partial y}\right)^2\right)$$

and the Jacobian determinant of F and H, a cubic form $G = G_F$ defined by

$$G = G_F(x,y) = \frac{\partial F}{\partial x}\frac{\partial H}{\partial y} - \frac{\partial F}{\partial y}\frac{\partial H}{\partial x}.$$

A quick computation reveals that, explicitly,

$$H = (b^2 - 3ac)x^2 + (bc - 9ad)xy + (c^2 - 3bd)y^2$$

and

$$\begin{aligned} G = \quad & (-27a^2d + 9abc - 2b^3)x^3 + (-3b^2c - 27abd + 18ac^2)x^2y \\ & + (3bc^2 - 18b^2d + 27acd)xy^2 + (-9bcd + 2c^3 + 27ad^2)y^3. \end{aligned}$$

These satisfy the syzygy

$$4H(x,y)^3 = G(x,y)^2 + 27D_F F(x,y)^2 \tag{5}$$

as well as the resultant identities:

$$\mathrm{Res}(F,G) = -8D_F^3 \quad \text{and} \quad \mathrm{Res}(F,H) = D_F^2. \tag{6}$$

Note here that we could just as readily work with $-G$ instead of G here (corresponding to taking the Jacobian determinant of H and F, rather than of F and H). Indeed, as we shall observe in Section 5.4, for our applications we will, in some sense, need to consider both possibilities.

Notice that if we set $(x,y) = (1,0)$ and multiply through by $\mathcal{D}^6/4$ (for any rational $\mathcal{D}$), then this syzygy can be rewritten as

$$(\mathcal{D}^2 H(1,0))^3 - \left(\frac{\mathcal{D}^3}{2}G(1,0)\right)^2 = 1728 \cdot \frac{\mathcal{D}^6 D_F}{256}F(1,0)^2.$$

Given an elliptic curve with corresponding invariants c_4, c_6, and Δ_E, we will show that it is always possible to construct a binary cubic form F, with corresponding $\mathcal{D}$ for which

$$\mathcal{D}^2 H(1,0) = c_4, \quad -\frac{1}{2}\mathcal{D}^3 G(1,0) = c_6 \quad \text{and} \quad \Delta_E = \frac{\mathcal{D}^6 D_F F(1,0)^2}{256}$$

(and hence equation (2) is satisfied). This is the basis of the proof of our main result, which provides an algorithm for computing all isomorphism classes of elliptic curves $E/\mathbb{Q}$ with conductor a fixed positive integer N. Though we state our result for curves with $j_E \neq 0$, the case $j_E = 0$ is easy to treat separately (see Section 3.1.7).

Theorem 1. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N = 2^\alpha 3^\beta N_0$, where N_0 is coprime to 6 and $0 \le \alpha \le 8$, $0 \le \beta \le 5$. Suppose further that $j_E \neq 0$. Then there exists an integral binary cubic form F of discriminant*

$$D_F = \mathrm{sign}(\Delta_E) 2^{\alpha_0} 3^{\beta_0} N_1,$$

and relatively prime integers u and v with

$$F(u,v) = \omega_0 u^3 + \omega_1 u^2 v + \omega_2 u v^2 + \omega_3 v^3 = 2^{\alpha_1} \cdot 3^{\beta_1} \cdot \prod_{p \mid N_0} p^{\kappa_p}, \tag{7}$$

such that E is isomorphic over $\mathbb{Q}$ to $E_{\mathcal{D}}$, where

$$E_{\mathcal{D}} \ : \ 3^{[\beta_0/3]} y^2 = x^3 - 27\mathcal{D}^2 H_F(u,v) x + 27\mathcal{D}^3 G_F(u,v) \tag{8}$$

and, for $[r]$ the greatest integer not exceeding a real number r,

$$\mathcal{D} = \prod_{p \mid \gcd(c_4(E), c_6(E))} p^{\min\{[\nu_p(c_4(E))/2], [\nu_p(c_6(E))/3]\}}. \tag{9}$$

The α_0, α_1, β_0, β_1, and N_1 are nonnegative integers satisfying $N_1 \mid N_0$,

$$(\alpha_0, \alpha_1) = \begin{cases} (2,0) \text{ or } (2,3) & \text{if } \alpha = 0, \\ (3, \ge 3) \text{ or } (2, \ge 4) & \text{if } \alpha = 1, \\ (2,1), (4,0) \text{ or } (4,1) & \text{if } \alpha = 2, \\ (2,1), (2,2), (3,2), (4,0) \text{ or } (4,1) & \text{if } \alpha = 3, \\ (2, \ge 0), (3, \ge 2), (4,0) \text{ or } (4,1) & \text{if } \alpha = 4, \\ (2,0) \text{ or } (3,1) & \text{if } \alpha = 5, \\ (2, \ge 0), (3, \ge 1), (4,0) \text{ or } (4,1) & \text{if } \alpha = 6, \\ (3,0) \text{ or } (4,0) & \text{if } \alpha = 7, \\ (3,1) & \text{if } \alpha = 8 \end{cases}$$

and

$$(\beta_0, \beta_1) = \begin{cases} (0,0) & \text{if } \beta = 0, \\ (0, \ge 1) \text{ or } (1, \ge 0) & \text{if } \beta = 1, \\ (3,0), (0, \ge 0) \text{ or } (1, \ge 0) & \text{if } \beta = 2, \\ (\beta, 0) \text{ or } (\beta, 1) & \text{if } \beta \ge 3. \end{cases}$$

The κ_p are nonnegative integers with

$$\nu_p(\Delta_E) = \begin{cases} \nu_p(D_F) + 2\kappa_p & \text{if } p \nmid \mathcal{D}, \\ \nu_p(D_F) + 2\kappa_p + 6 & \text{if } p \mid \mathcal{D} \end{cases} \tag{10}$$

and

$$\kappa_p \in \{0,1\} \quad \text{whenever} \quad p^2 \mid N_1. \tag{11}$$

Further, we have

$$\text{if} \quad \beta_0 \ge 3, \quad \text{then} \quad 3 \mid \omega_1 \text{ and } 3 \mid \omega_2, \tag{12}$$

and

$$\text{if } \nu_p(N) = 1, \text{ for } p \ge 3, \text{ then } p \mid D_F F(u,v). \tag{13}$$

Here, as we shall make explicit in the next subsection, the form F corresponding to the curve E in Theorem 1 determines the 2-division field of E. This connection was noted by Rubin and Silverberg [55] in a somewhat different context—they proved that if K is a field of characteristic $\neq 2, 3$, $F(u, v)$ is a binary cubic form defined over K, E is an elliptic curve defined by $y^2 = F(x, 1)$, and E_0 is another elliptic curve over K with the property that $E[2] \cong E_0[2]$ (as Galois modules), then E_0 is isomorphic to the curve

$$y^2 = x^3 - 3H_F(u, v)x + G_F(u, v),$$

for some $u, v \in K$. We thank the referee for bringing this paper to our attention.

3.1. **Remarks.** Before we proceed, there are a number of observations we should make regarding Theorem 1.

3.1.1. *Historical comments.* Theorem 1 is based upon a generalization of classical work of Mordell [45] (see also Theorem 3 of Chapter 24 of Mordell [46]), in which the Diophantine equation

$$X^2 + kY^2 = Z^3$$

is treated through reduction to binary cubic forms and their covariants, under the assumption that X and Z are coprime. That this last restriction can, with some care, be eliminated, was noted by Sprindzuk (see Chapter VI of [62]). A similar approach to this problem can be made through the invariant theory of binary quartic forms, where one is led to solve, instead, equations of the shape

$$X^2 + kY^3 = Z^3.$$

We will not carry out the analogous analysis here.

3.1.2. *2-division fields and reducible forms.* It might happen that the form F whose existence is guaranteed by Theorem 1 is reducible over $\mathbb{Z}[x, y]$. This occurs precisely when the elliptic curve E has a nontrivial rational 2-torsion point. This follows from the more general fact that the cubic form $F(u, v) = \omega_0 u^3 + \omega_1 u^2 v + \omega_2 uv^2 + \omega_3 v^3$ corresponding to an elliptic curve E has the property that the splitting field of $F(u, 1)$ is isomorphic to the 2-division field of E. This is almost immediate from the identity

$$\begin{aligned} 3^3\,\omega_0^2\,F\left(\tfrac{x-\omega_1}{3\omega_0}, 1\right) &= x^3 + (9\omega_0\omega_2 - 3\omega_1^2)x + 27\omega_0^2\omega_3 - 9\omega_0\omega_1\omega_2 + 2\omega_1^3 \\ &= x^3 - 3H_F(1, 0)x + G_F(1, 0). \end{aligned}$$

Indeed, from (8), the elliptic curve defined by the equation $y^2 = x^3 - 3H_F(1, 0)x + G_F(1, 0)$ is a quadratic twist of that given by the model $y^2 = x^3 - 27c_4(E)x - 54c_6(E)$, and hence also of E (whereby they have the same 2-division field).

3.1.3. *Imprimitive forms.* It is also the case that the cubic forms arising need not be primitive (in the sense that $\gcd(\omega_0, \omega_1, \omega_2, \omega_3) = 1$). This situation can occur if each of the coefficients of F is divisible by some integer $g \in \{2, 3, 6\}$. Since the discriminant is a quartic form in the coefficients of F, for this to take place one requires that

$$D_F \equiv 0 \pmod{g^4}.$$

This is a necessary but not sufficient condition for the form F to be imprimitive. It follows, if we wish to restrict attention to primitive forms in Theorem 1, that the possible values for $\nu_p(D_F)$ that can arise are

(14)
$$\nu_2(D_F) \in \{0,2,3,4\}, \quad \nu_3(D_F) \in \{0,1,3,4,5\} \quad \text{and} \quad \nu_p(D_F) \in \{0,1,2\} \ \text{ for } p > 3.$$

3.1.4. *Possible twists.* We note that necessarily

$$\mathcal{D} \mid 2^3 \cdot 3^2 \cdot \prod_{p \mid N_0} p, \tag{15}$$

so that, given N, there is a finite set of $E_{\mathcal{D}}$ to consider (we can restrict our attention to quadratic twists of the curve defined via $y^2 = x^3 - 3H_F(1,0)x + G_F(1,0)$, by squarefree divisors of $6N$). In case we are dealing with the squarefree conductor N (i.e., for semistable curves E), then, from Tables 1, 2, and 3, it follows that $\mathcal{D} \in \{1,2\}$.

3.1.5. *Necessity, but not sufficiency.* If we search for elliptic curves of conductor N, say, there may exist a cubic form F for which the corresponding Thue-Mahler equation (7) has a solution, where all of the conditions of Theorem 1 are satisfied, but for which the corresponding $E_{\mathcal{D}}$ has conductor $N_{E_{\mathcal{D}}} \neq N$ for all possible $\mathcal{D}$. This can happen when certain local conditions at primes dividing $6N$ are not met; these local conditions are, in practice, easy to check and only a minor issue when performing computations. Indeed, when producing tables of elliptic curves of conductor up to some given bound, we will, in many cases, apply Theorem 1 to find all curves with good reduction outside a fixed set of primes—in effect, working with multiple conductors simultaneously. For such a computation, the conductor of every twist $E_{\mathcal{D}}$ we encounter will be of interest to us.

3.1.6. *Special binary cubic forms.* If, for a given binary form $F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, 3 divides both the coefficients b and c (say $b = 3b_0$ and $c = 3c_0$), then $27 \mid D_F$ and, consequently, we can write $D_F = 27\widetilde{D}_F$, where

$$\widetilde{D}_F = -a^2d^2 + 6ab_0c_0d + 3b_0^2c_0^2 - 4ac_0^3 - 4b_0^3d.$$

One can show that the set of binary cubic forms with $b \equiv c \equiv 0 \pmod 3$ is closed within the larger set of all binary cubic forms in $\mathbb{Z}[x,y]$, under the action of either $\mathrm{SL}_2(\mathbb{Z})$ or $\mathrm{GL}_2(\mathbb{Z})$. Also note that for such forms we have

$$\widetilde{H}_F(x,y) = \frac{H_F(x,y)}{9} = (b_0^2 - ac_0)x^2 + (b_0c_0 - ad)xy + (c_0^2 - b_0d)y^2$$

and $\widetilde{G}_F(x,y) = G_F(x,y)/27$, so that

$$\begin{aligned}\widetilde{G}_F(x,y) = {} & (-a^2d + 3ab_0c_0 - 2b_0^3)x^3 + 3(-b_0^2c_0 - ab_0d + 2ac_0^2)x^2y \\ & + 3(b_0c_0^2 - 2b_0^2d + ac_0d)xy^2 + (-3b_0c_0d + 2c_0^3 + ad^2)y^3.\end{aligned}$$

The syzygy now becomes

$$4\widetilde{H}_F(x,y)^3 = \widetilde{G}_F(x,y)^2 + \widetilde{D}_F F(x,y)^2. \tag{16}$$

We note, from Theorem 1, that we will be working exclusively with forms of this shape whenever we wish to treat elliptic curves of conductor $N \equiv 0 \pmod{3^3}$.

3.1.7. *The case $j_E = 0$.* This case is treated over a general number field in Proposition 4.1 of Cremona and Lingham [19]. The elliptic curves $E/\mathbb{Q}$ with $j_E = 0$ and a given conductor N are particularly easy to determine, since a curve with this property is necessarily isomorphic over $\mathbb{Q}$ to a *Mordell* curve with a model of the shape $Y^2 = X^3 - 54c_6$, where $c_6 = c_6(E)$. Such a model is minimal except possibly at 2 and 3 and has discriminant $-2^6 \cdot 3^9 \cdot c_6^2$ (whereby any primes $p > 2$ which divide c_6 necessarily also divide N). Here, without loss of generality, we may suppose that c_6 is sixth-power-free. Further, from Tables 1, 2, and 3, we have that $\nu_2(N) \in \{0, 2, 3, 4, 6\}$, that $\nu_3(N) \in \{2, 3, 5\}$, and that $\nu_p(N) = 2$ whenever $p \mid N$ for $p > 3$. Given a positive integer N satisfying these constraints, it is therefore a simple matter to check to see if there are elliptic curves $E/\mathbb{Q}$ with conductor N and j-invariant 0. One needs only to compute the conductors of the curves given by $Y^2 = X^3 - 54c_6$ for each sixth-power-free integer (positive or negative) c_6 dividing $64N^3$.

3.2. **The algorithm.** It is straightforward to convert Theorem 1 into an algorithm for finding all $E/\mathbb{Q}$ of conductor N. We can proceed as follows.

(1) Begin by finding all $E/\mathbb{Q}$ of conductor N with $j_E = 0$, as outlined in Section 3.1.7.
(2) Next, compute $\mathrm{GL}_2(\mathbb{Z})$-representatives for every binary form F with discriminant

$$\Delta_F = \pm 2^{\alpha_0} 3^{\beta_0} N_1$$

for each divisor N_1 of N_0, and each possible pair (α_0, β_0) given in the statement of Theorem 1 (see (14) for specifics). We describe an algorithm for listing these forms in Section 5.
(3) Solve the corresponding Thue-Mahler equations, finding pairs of integers (u, v) such that $F(u, v)$ is an S-unit, where $S = \{p \text{ prime } : p \mid N\} \cup \{2\}$ and $F(u, v)$ satisfies the additional conditions given in the statement of Theorem 1.
(4) For each cubic form F and pair of integers (u, v), consider the elliptic curve

$$E_1 \quad : \quad y^2 = x^3 - 27H_F(u, v)x + 27G_F(u, v)$$

and all its quadratic twists by squarefree divisors of $6N$. Output those curves with conductor N (if any).

The first, second, and fourth steps here are straightforward; the first and second can be done efficiently, while the fourth is essentially trivial. The main bottleneck is step (3). While there is a deterministic procedure for carrying this out (see Tzanakis and de Weger [68], [69]), it is both involved and, often, computationally taxing. An earlier implementation of this method in Magma due to Hambrook [31] has subsequently been refined by the second author [28]; the most up-to-date version of this code (which we will reference here and henceforth as UBC-TM) is available at

`http://www.nt.math.ubc.ca/BeGhRe/Code/UBC-TMCode`.

We give a number of examples of this general procedure in Section 6. In Section 7, we show that in the special cases where the conductor is prime or the square of a prime, the Thue-Mahler equations (7) (happily) reduce to Thue equations (i.e., the exponents on the right-hand side of (7) are absolutely bounded). This situation occurs because, for such elliptic curves, a very strong form of Szpiro's conjecture (bounding the minimal discriminant of an elliptic curve from above in terms of its conductor) is known to hold. Thue equations can be solved by routines that are computationally much easier than is currently the case for Thue-Mahler equations; such procedures have been implemented in Pari/GP [50] and Magma [9]. Further, in this situation, it is possible to apply a much more computationally efficient argument to find all such elliptic curves heuristically but not, perhaps, completely (see Section 8).

4. Proof of Theorem 1

Proof. Given an elliptic curve $E/\mathbb{Q}$ of conductor $N = 2^{\alpha}3^{\beta}N_0$ and invariants $c_4 = c_4(E) \neq 0$ and $c_6 = c_6(E)$, we will construct a corresponding cubic form F explicitly. In fact, our form F will have the property that its leading coefficient will be supported on the primes dividing $6N$, i.e., that

$$F(1,0) = 2^{\alpha_1} \cdot 3^{\beta_1} \cdot \prod_{p \mid N_0} p^{\kappa_p}.$$

Define $\mathcal{D}$ as in (9), i.e., take $\mathcal{D}$ to be the largest integer whose square divides c_4 and whose cube divides c_6. We then set

$$X = c_4/\mathcal{D}^2 \quad \text{and} \quad Y = c_6/\mathcal{D}^3,$$

whereby, from (2),

$$Y^2 = X^3 + (-1)^{\delta+1}M \tag{17}$$

for

$$M = \mathcal{D}^{-6} \cdot 2^6 \cdot 3^3 \cdot |\Delta_E|.$$

Note that the assumption that $c_4(E) \neq 0$ ensures that both the j-invariant $j_E \neq 0$ and that $X \neq 0$.

It will prove useful to us later to understand precisely the possible common factors among $X, Y, \mathcal{D}$, and M. For any $p > 3$, we have $\nu_p(N) \leq 2$. When $\nu_p(N) = 1$, from Table 3 we find that

$$(\nu_p(\mathcal{D}), \nu_p(X), \nu_p(Y), \nu_p(M)) = (0, 0, 0, \geq 1), \tag{18}$$

while, if $\nu_p(N) = 2$, then either

$$\nu_p(\mathcal{D}) = 1 \text{ and } \min\{\nu_p(X), \nu_p(Y)\} = 0,\ \nu_p(M) = 0 \tag{19}$$

or

$$\nu_p(\mathcal{D}) \leq 1,\ (\nu_p(X), \nu_p(Y), \nu_p(M)) = (0, 0, \geq 1), (\geq 1, 1, 2), (1, \geq 2, 3) \text{ or } (\geq 2, 2, 4). \tag{20}$$

Things are rather more complicated for the primes 2 and 3; we summarize this in Tables 4 and 5 (which are, in turn, compiled from the data in Tables 1 and 2).

TABLE 4. The possible values of $\nu_2(N), \nu_2(X), \nu_2(Y), \nu_2(M)$ and $\nu_2(D)$

$\nu_2(N)$	$(\nu_2(X), \nu_2(Y), \nu_2(M), \nu_2(\mathcal{D}))$
0	$(\geq 2, 0, 0, 1)$ or $(0, 0, 6, 0)$
1	$(0, 0, \geq 7, 0)$
2	$(\geq 2, 2, 4, 1), (\geq 2, 1, 2, 2)$ or $(0, 0, 2, 2)$
3	$(\geq 2, 2, 4, 1), (\geq 2, 1, 2, 2)$ or $(0, 0, t, 2), t = 2, 4$ or 5
4	$(\geq 2, 2, 4, 1), (\geq 2, 1, 2, 2), (\geq 2, 0, 0, 3)$ or $(0, 0, t, 2), t = 2$ or $t \geq 4$
5	$(\geq 0, \geq 0, 0, 2), (0, \geq 0, 0, 3), (0, 0, 3, 2)$ or $(1, 0, 0, 3)$
6	$(\geq 0, \geq 0, 0, 2), (0, \geq 0, 0, 3), (\geq 2, 2, 4, 2), (\geq 2, 1, 2, 3)$ or $(0, 0, \geq 2, 3)$
7	$(0, 0, 1, 2), (0, 0, 1, 3), (1, 1, 2, 2)$ or $(1, 1, 2, 3)$
8	$(1, \geq 2, 3, 2)$ or $(1, \geq 2, 3, 3)$.

TABLE 5. The possible values of $\nu_3(N), \nu_3(X), \nu_3(Y), \nu_3(M)$, and $\nu_3(D)$

$\nu_3(N)$	$(\nu_3(X), \nu_3(Y), \nu_3(M), \nu_3(\mathcal{D}))$
0	$(1, \geq 3, 3, 0)$ or $(0, 0, 3, 0)$
1	$(0, 0, \geq 4, 0)$
2	$(\geq 0, 0, 0, 1), (0, \geq 2, 0, 1), (0, 0, \geq 3, 1), (1, \geq 3, 3, 1), (\geq 0, 0, 0, 2)$ or $(0, \geq 2, 0, 2)$
3	$(\geq 0, 0, 0, 1), (\geq 0, 0, 0, 2), (0, 1, 0, 1), (0, 1, 0, 2), (0, 0, 2, 1)$ or $(0, 0, 2, 2)$
4	$(0, 0, 1, 1), (0, 0, 1, 2), (1, 2, 3, 1)$ or $(1, 2, 3, 2)$
5	$(\geq 1, 1, 2, 1), (\geq 1, 1, 2, 2), (\geq 2, 2, 4, 1)$ or $(\geq 2, 2, 4, 2)$.

We will construct a cubic form

$$F_1(x, y) = ax^3 + 3b_0x^2y + 3c_0xy^2 + dy^3,$$

one coefficient at a time; our main challenge will be to ensure that the a, b_0, c_0 and d we produce are actually integral rather than just rational. The form F whose existence is asserted in the statement of Theorem 1 will turn out to be either F_1 or $F_1/3$.

Let us write

$$M = M_1 \cdot M_2,$$

where M_2 is the largest integer divisor of M that is coprime to X, so that

$$M_1 = \prod_{p \mid X} p^{\nu_p(M)} \quad \text{and} \quad M_2 = \prod_{p \nmid X} p^{\nu_p(M)}.$$

We define

$$a_1 = \prod_{p \mid M_1} p^{\left[\frac{\nu_p(M)-1}{2}\right]} \tag{21}$$

and set

$$a_2 = \begin{cases} 3^{-1} \prod_{p \mid M_2} p^{\left[\frac{\nu_p(M)}{2}\right]} & \text{if } \nu_3(X) = 0,\ \nu_3(M) = 2t,\ t \in \mathbb{Z}, t \geq 2, \\ \prod_{p \mid M_2} p^{\left[\frac{\nu_p(M)}{2}\right]} & \text{otherwise.} \end{cases} \tag{22}$$

Define $a = a_1 \cdot a_2$. It follows that $a_1^2 \mid M_1$ and, from (18), (19), (20), and Tables 4 and 5, that both

$$a_1 \mid X \quad \text{and} \quad a_1^2 \mid Y.$$

We write $X = a_1 \cdot X_1$ and observe that $a_2^2 \mid M_2$. Note that a_2 is coprime to X and hence to a_1. Since $a^2 \mid M$, we may thus define a positive integer K via $K = M/a^2$, so that (17) becomes

$$Y^2 - X^3 = (-1)^{\delta+1} K a^2.$$

From the fact that $\gcd(a_2, X) = 1$ and $X \neq 0$, we may choose B so that

$$a_2 B \equiv -Y/a_1 \pmod{X^3},$$

whereby

$$aB + Y \equiv 0 \pmod{a_1 X^3}. \tag{23}$$

Note that, since $a_1^2 \mid Y$ and $a_1 \mid X$, it follows that $a_1 \mid B$. Let us define

$$b_0 = \frac{aB+Y}{X}, \quad c_0 = \frac{b_0^2 - X}{a}, \quad \text{and} \quad d = \frac{b_0 c_0 - 2B}{a}. \tag{24}$$

We now demonstrate that these are all integers. That $b_0 \in \mathbb{Z}$ is immediate from (23). Since $b_0 X - Y = aB$, we know that $b_0 X \equiv Y \pmod{a}$. Squaring both sides thus gives

$$b_0^2 X^2 \equiv Y^2 \equiv X^3 + (-1)^{\delta+1} K a^2 \equiv X^3 \pmod{a_1 \cdot a_2},$$

and, since $\gcd(a_2, X) = 1$,

$$b_0^2 \equiv X \pmod{a_2}.$$

From (23), we have $b_0 \equiv 0 \pmod{a_1 X^2}$, whereby, since $a_1 \mid X$,

$$b_0^2 \equiv X \equiv 0 \pmod{a_1}.$$

The fact that $\gcd(a_1, a_2) = 1$ thus allows us to conclude that $b_0^2 \equiv X \pmod{a}$ and hence that $c_0 \in \mathbb{Z}$.

It remains to show that d is an integer. Let us rewrite ad as

$$ad = b_0 c_0 - 2B = \left(\frac{aB+Y}{aX}\right)\left(\left(\frac{aB+Y}{X}\right)^2 - X\right) - 2B,$$

so that

$$ad = \left(\frac{aB+Y}{aX}\right)\left(\frac{(-1)^{\delta+1} K a^2 + 2aBY + a^2 B^2}{X^2}\right) - 2B.$$

Expanding, we find that

$$X^3 d = (-1)^{\delta+1} KY + 3YB^2 + aB^3 + (-1)^{\delta+1} 3KaB. \tag{25}$$

We wish to show that

$$(-1)^{\delta+1} KY + 3YB^2 + aB^3 + (-1)^{\delta+1} 3KaB \equiv 0 \pmod{X^3}.$$

From (23), we have that

$$(-1)^{\delta+1} KY + 3YB^2 + aB^3 + (-1)^{\delta+1} 3KaB \equiv 2Y\left(B^2 + (-1)^{\delta} K\right) \pmod{a_1 X^3}.$$

Multiplying congruence (23) by $aB - Y$ (which, from our prior discussion, is divisible by a_1^2), we find that

$$a^2 B^2 \equiv Y^2 \equiv X^3 + (-1)^{\delta+1} K a^2 \pmod{a_1^3 X^3}$$

and hence, dividing through by a_1^2,

$$a_2^2 B^2 \equiv a_1 X_1^3 + (-1)^{\delta+1} K a_2^2 \pmod{a_1 X^3}.$$

It follows that

$$B^2 + (-1)^\delta K \equiv a_2^{-2} a_1 X_1^3 \pmod{a_1 X^3}, \tag{26}$$

and so, since $a_1^2 \mid Y$,

$$Y\left(B^2 + (-1)^\delta K\right) \equiv 0 \pmod{X^3},$$

whence we conclude that d is an integer, as desired.

With these values of a, b_0, c_0, and d, we can then confirm (with a quick computation) that the cubic form

$$F_1(x,y) = ax^3 + 3b_0x^2y + 3c_0xy^2 + dy^3$$

has discriminant

$$D_{F_1} = \frac{108}{a^2}(X^3 - Y^2) = (-1)^\delta \cdot 2^2 \cdot 3^3 \cdot K.$$

We also note that

$$F_1(1,0) = a, \quad \widetilde{H}_{F_1}(1,0) = b_0^2 - ac_0 = X$$

and

$$-\frac{1}{2}\widetilde{G}_{F_1}(1,0) = \frac{1}{2}(a^2d - 3ab_0c_0 + 2b_0^3) = Y,$$

where $\widetilde{G}_F$ and $\widetilde{H}_F$ are as in Section 3.1.6.

Summarizing Table 5, we find that we are in one of the following four cases:

(i) $\nu_3(X) = 1$, $\nu_3(Y) = 2$, $\nu_3(M) = 3$, and $\nu_3(N) = 4$,
(ii) $\nu_3(X) \geq 2$, $\nu_3(Y) = 2$, $\nu_3(M) = 4$, $\nu_3(N) = 5$,
(iii) $\nu_3(M) \leq 2$ and $\nu_3(N) \geq 2$, or
(iv) $\nu_3(M) \geq 3$ and either $\nu_3(XY) = 0$ or $\nu_3(X) = 1$, $\nu_3(Y) \geq 3$.

In cases (i), (ii), and (iii), we choose $F = F_1$, i.e.,

$$(\omega_0, \omega_1, \omega_2, \omega_3) = (a, 3b_0, 3c_0, d),$$

so that

$$F(1,0) = a, \quad D_F = (-1)^\delta 2^2 \cdot 3^3 \cdot K, \quad c_4 = \mathcal{D}^2 \widetilde{H}_F(1,0) \quad \text{and} \quad c_6 = -\frac{1}{2}\mathcal{D}^3 \widetilde{G}_F(1,0).$$

It follows that E is isomorphic over $\mathbb{Q}$ to the curve

$$y^2 = x^3 - 27c_4x - 54c_6 = x^3 - 3\mathcal{D}^2 H_F(1,0)x + \mathcal{D}^3 G_F(1,0).$$

In case (iv), observe that, from definitions (21) and (22),

$$\nu_3(a) = \left[\frac{\nu_3(M) - 1}{2}\right] \quad \text{and} \quad \nu_3(K) = \nu_3(M) - 2\nu_3(a), \tag{27}$$

so that $3 \mid a$ and $3 \mid K$. From equation (25), $3 \mid X^3 d$. If $\nu_3(X) = 0$ this implies that $3 \mid d$. On the other hand, if $\nu_3(X) = 1$, then, from (26), we may conclude that $3 \mid B$. Since each of a, B and K is divisible by 3, while $\nu_3(X) = 1$ and $\nu_3(Y) \geq 3$, equation (25) once again implies that $3 \mid d$. In this case, we can therefore write $a = 3a_0$ and $d = 3d_0$, for integers a_0 and d_0 and set $F = F_1/3$, i.e., take

$$(\omega_0, \omega_1, \omega_2, \omega_3) = (a_0, b_0, c_0, d_0).$$

We have

$$F(1,0) = a/3, \quad D_F = (-1)^\delta 2^2 \cdot K/3, \quad c_4 = \mathcal{D}^2 H_F(1,0) \quad \text{and} \quad c_6 = -\frac{1}{2}\mathcal{D}^3 G_F(1,0).$$

The curve E is now isomorphic over $\mathbb{Q}$ to the model

$$y^2 = x^3 - 27c_4 x - 54c_6 = x^3 - 27\mathcal{D}^2 H_F(1,0)x + 27\mathcal{D}^3 G_F(1,0).$$

Since $|D_F|/D_F = (-1)^\delta$ and $a^2 K \mid 1728\Delta_E$, we may write

$$F(1,0) = 2^{\alpha_1} \cdot 3^{\beta_1} \cdot \prod_{p \mid N_0} p^{\kappa_p} \quad \text{and} \quad D_F = (|\Delta_E|/\Delta_E) 2^{\alpha_0} 3^{\beta_0} N_1,$$

for nonnegative integers $\alpha_0, \alpha_1, \beta_0, \beta_1, \kappa_p$ and a positive integer N_1, divisible only by primes dividing N_0. More explicitly, we have

$$\alpha_0 = \nu_2(K) + 2 \quad \text{and} \quad \beta_0 = \nu_3(K) + \begin{cases} 3 & \text{in case (i), (ii) or (iii), or} \\ -1 & \text{in case (iv),} \end{cases}$$

and

$$\alpha_1 = \nu_2(a) \quad \text{and} \quad \beta_1 = \nu_3(a) + \begin{cases} 0 & \text{in case (i), (ii) or (iii), or} \\ -1 & \text{in case (iv).} \end{cases}$$

It remains for us to prove that these integers satisfy the conditions listed in the statement of the theorem. It is straightforward to check this, considering in turn each possible triple (X, Y, M) from (18), (19), (20), and Tables 4 and 5, and using the fact that $K = M/a^2$.

In particular, if $p > 3$, we have $\nu_p(\Delta_E) = 6\nu_p(\mathcal{D}) + \nu_p(D_F) + 2\kappa_p$. From Table 3 and (9), we have $\nu_p(\mathcal{D}) \leq 1$, whereby (10) follows. Further,

$$\nu_p(a) = \begin{cases} \left[\frac{\nu_p(M)-1}{2}\right] & \text{if } p \mid X, \\ \left[\frac{\nu_p(M)}{2}\right] & \text{if } p \nmid X, \end{cases} \tag{28}$$

and so, if $p \nmid X$,

$$\nu_p(M) - 2\nu_p(a) \leq 1.$$

Since $a^2 K = M$, if $p^2 \mid D_F$, then $\nu_p(N) = 2$ and it follows that we are in case (20), with $p \mid X$. We may thus conclude that $\nu_p(M) \in \{2, 3, 4\}$ and hence, from (28), that $\nu_p(a) \leq 1$. This proves (11).

For (12), note that, in cases (i), (ii), and (iii), we clearly have that $3 \mid \omega_1$ and $3 \mid \omega_2$. In case (iv), from (27),

$$\beta_0 = \nu_3(D_F) = \nu_3(K) - 1 = \nu_3(M) - 2\left[\frac{\nu_3(M) - 1}{2}\right] - 1 \in \{0, 1\}.$$

Finally, to see (13), note that if $\nu_p(N) = 1$, for $p > 3$, then we have (18) and hence

$$\nu_p(D_F) + 2\nu_p(F(u,v)) = \nu_p(M) \geq 1,$$

whereby $p \mid D_F$ or $p \mid F(u,v)$. We may also readily check that the same conclusion obtains for $p = 3$ (since, equivalently, $\beta_0 + \beta_1 \geq 1$). This completes the proof of Theorem 1. □

To illustrate this argument, suppose we consider the elliptic curve (denoted 109a1 in Cremona's database) defined via

$$E \ : \ y^2 + xy = x^3 - x^2 - 8x - 7,$$

with $\Delta_E = -109$. We have

$$c_4(E) = 393 \quad \text{and} \quad c_6(E) = 7803,$$

so that $\gcd(c_4(E), c_6(E)) = 3$. It follows that

$$\mathcal{D} = 1,\ X = 393,\ Y = 7803,\ \delta = 1,\ M = 2^6 \cdot 3^3 \cdot 109,$$

and hence we have

$$M_1 = 3^3,\ M_2 = 2^6 \cdot 109,\ a_1 = 3,\ a_2 = 2^3,\ a = 2^3 \cdot 3, \text{ and } K = 3 \cdot 109.$$

We solve the congruence $8B \equiv -2601 \pmod{393^3}$ to find that we may choose $B = 7586982$, so that

$$b_0 = 463347, \quad c_0 = 8945435084 \quad \text{and} \quad d = 172701687278841.$$

We are in case (iv) and thus set

$$F(x, y) = 8x^3 + 463347x^2y + 8945435084xy^2 + 57567229092947y^3,$$

with discriminant $D_F = -4 \cdot 109$,

$$G_F(1, 0) = -15606 = -2c_6(E) \quad \text{and} \quad H_F(1, 0) = 393 = c_4(E).$$

The curve E is thus isomorphic to the model

$$E_{\mathcal{D}} \ : \ y^2 = x^3 - 27\mathcal{D}^2 H_F(1, 0)x + 27\mathcal{D}^3 G_F(1, 0) = x^3 - 10611x - 421362. \tag{29}$$

We observe that the form F is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to a "reduced" form (see Section 5 for details), given by

$$\tilde{F}(x, y) = x^3 + 3x^2y + 4xy^2 + 6y^3.$$

In fact, this is the only form (up to $\mathrm{GL}_2(\mathbb{Z})$-equivalence) of discriminant $\pm 4 \cdot 109$. We can check that the solutions to the Thue equation $\tilde{F}(u, v) = 8$ are given by $(u, v) = (2, 0)$ and $(u, v) = (-7, 3)$. The minimal quadratic twist of

$$y^2 = x^3 - 27H_{\tilde{F}}(2, 0)x + 27G_{\tilde{F}}(2, 0)$$

has conductor $2^5 \cdot 109$ and hence cannot correspond to E. For the solution $(u, v) = (-7, 3)$, we find that the curve given by the model

$$y^2 = x^3 - 27H_{\tilde{F}}(-7, 3)x + 27G_{\tilde{F}}(-7, 3) = x^3 - 10611x + 421362,$$

is the quadratic twist by -1 of the curve (29). This situation arises from the fact that G_F is an $\mathrm{SL}_2(\mathbb{Z})$-covariant, but not a $\mathrm{GL}_2(\mathbb{Z})$-covariant of F (we will discuss this more in the next section).

5. Finding representative forms

As Theorem 1 illustrates, we are able to tabulate elliptic curves over $\mathbb{Q}$ with good reduction outside a given set of primes, by finding a set of representatives for $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of binary cubic forms with certain discriminants, and then solving a number of Thue-Mahler equations. In this section, we will provide a brief description of techniques to find distinguished *reduced* representatives for equivalence classes of cubic forms over a given range of discriminants. For both positive and negative discriminants, the notion of *reduction* arises from associating a particular definite quadratic form to a given cubic form.

5.1. **Irreducible forms.** For forms of positive discriminant, there is a well developed classical theory of reduction dating back to work of Hermite [33], [34] and, later, Davenport (see, e.g., [20], [21], and [23]). We can actually apply this method to both reducible and irreducible forms. Initially, though, we will assume the forms are irreducible, since we will treat the elliptic curves corresponding to reducible forms by a somewhat different approach (see Section 5.2). Note that when one speaks of "irreducible, reduced forms", as Davenport observes, "the terminology is unfortunate, but can hardly be avoided" ([22], p. 184).

In each of Belabas [3], Belabas and Cohen [4], and Cremona [17], we find very efficient algorithms for computing cubic forms of both positive and negative discriminant, refining classical work of Hermite, Berwick and Mathews [42], and Julia [35]. These are readily translated into computer code to loop over valid (a, b, c, d)-values (with corresponding forms $ax^3+bx^2y+cxy^2+dy^3$). The running time in each case is linear in the upper bound X. Realistically, this step (finding representatives for our cubic forms) is highly unlikely to be the bottleneck in our computations.

5.2. **Reducible forms.** One can make similar definitions of reduction for reducible forms (see [5] for example). However, for our purposes, it is sufficient to note that a reducible form is equivalent to

$$F(x, y) = bx^2y + cxy^2 + dy^3 \quad \text{with} \quad 0 \le d \le c,$$

which has discriminant

$$\Delta_F = b^2(c^2 - 4bd).$$

To find all elliptic curves with good reduction outside $S = \{p_1, p_2, \dots, p_k\}$, corresponding to reducible cubics in Theorem 1 (i.e., those E with at least one rational 2-torsion point), it is enough to find all such triples (b, c, d) for which there exist integers x and y so that both

$$b^2(c^2 - 4bd) \quad \text{and} \quad bx^2y + cxy^2 + dy^3$$

are S^*-units (with $S^* = S \cup \{2\}$). For this to be true, it is necessary that each of the integers

$$b, \quad c^2 - 4bd, \quad y, \quad \text{and} \quad \mu = bx^2 + cxy + dy^2$$

is an S^*-unit. Taking the discriminant of μ as a function of x, we thus require that

$$(c^2 - 4bd)y^2 + 4b\mu = Z^2, \tag{30}$$

for some integer Z. This is an equation of the shape

$$X + Y = Z^2 \tag{31}$$

in S^*-units X and Y.

An algorithm for solving such equations is described in detail in Chapter 7 of de Weger [71] (see also [72]); it relies on bounds for linear forms in p-adic and complex logarithms and various reduction techniques from Diophantine approximation. An implementation of this is available at

`http://www.nt.math.ubc.ca/BeGhRe/Code/UBC-TMCode`.

While a priori equation (31) arises as only a necessary condition for the existence of an elliptic curve of the desired form, given any solution to (31) in S^*-units X and Y and integer Z, the curves

$$E_1(X, Y) \quad : \quad y^2 = x^3 + Zx^2 + \frac{X}{4}x$$

and

$$E_2(X,Y) \quad : \quad y^2 = x^3 + Zx^2 + \frac{Y}{4}x$$

have nontrivial rational 2-torsion (i.e., the point corresponding to $(x,y) = (0,0)$) and discriminant X^2Y and XY^2, respectively (and hence good reduction at all primes outside S^*).

Though a detailed analysis of running times for solving equations of the shape (31), or for solving more general cubic Thue-Mahler equations, has not to our knowledge been carried out, our experience from carrying out such computations for several thousand sets S is that, typically, the former can be done significantly faster than the latter. By way of example, solving (31) for $S = \{2,3,5,7,11\}$ takes only a few hours on a laptop, while treating the analogous problem of determining all elliptic curves over $\mathbb{Q}$ with trivial rational 2-torsion and good reduction outside S (see Section 6.4) requires many thousand machine-hours.

5.3. **Computing forms of fixed discriminant.** For our purposes, we will typically compute and tabulate a large list of irreducible forms of absolute discriminant bounded by a given positive number X (of size up to 10^{12} or so, beyond which storage becomes problematical). In certain situations, however, we will want to compute all forms of a given fixed, larger discriminant (perhaps up to size 10^{15}). To carry this out and find desired forms of the shape $ax^3 + bx^2y + cxy^2 + dy^3$, we can argue as in, for example, Cremona [17], to restrict our attention to $O(X^{3/4})$ triples (a,b,c). From (4), the definition of D_F, we have that

$$d = \frac{9abc - 2b^3 \pm \sqrt{4(b^2-3ac)^3 - 27a^2D_F}}{27a^2}$$

and hence it remains to check that the quantity $4(b^2-3ac)^3 - 27a^2D_F$ is an integer square, that the relevant conditions modulo $27a^2$ are satisfied, and that a variety of further inequalities from [17] are satisfied. The running time for finding forms with discriminants of absolute value of size X via this approach is of order $X^{3/4}$.

5.4. **$\mathbf{GL}_2(\mathbb{Z})$ vs $\mathbf{SL}_2(\mathbb{Z})$.** One last observation which is very important to make before we proceed, is that while G_F^2 is $\mathrm{GL}_2(\mathbb{Z})$-covariant, the same is not actually true for G_F (it is, however, an $\mathrm{SL}_2(\mathbb{Z})$-covariant). This may seem like a subtle point, but what it means for us in practice is that, having found our $\mathrm{GL}_2(\mathbb{Z})$-representative forms F and corresponding curves of the shape $E_{\mathcal{D}}$ from Theorem 1, we need, in every case, to also check to see if

$$\tilde{E}_{\mathcal{D}} \quad : \quad 3^{[\beta_0/3]}y^2 = x^3 - 27\mathcal{D}^2H_F(u,v)x - 27\mathcal{D}^3G_F(u,v),$$

the quadratic twist of $E_{\mathcal{D}}$ by -1, yields a curve of the desired conductor.

6. Examples

In this section, we will describe a few applications of Theorem 1 to computing all elliptic curves of a fixed conductor N, or all curves with good reduction outside a given set of primes S. We restrict our attention to examples with composite conductors, since the case of conductors p and p^2, for p prime, will be treated at length in Section 7 (and subsequently). For the examples in Sections 6.1, 6.2.1, 6.2.2, and 6.2.3, since the conductors under discussion are not "square-full", there are necessarily no curves E encountered with $j_E = 0$.

In our computations in this section, we executed all jobs in parallel via the shell tool [65]. We note that our Magma code lends itself easily to parallelization, and we made full use of this fact throughout.

We carried out a one-time computation of all irreducible cubic forms that can arise in Theorem 1, of an absolute discriminant bounded by 10^{10}. This computation took slightly more than 3 hours on a cluster of 40 cores; roughly half this time was taken up with sorting and organizing output files. There are 996198693 classes of irreducible cubic forms of positive discriminant and 3079102475 of negative discriminant in the range in question; storing them requires roughly 120 gigabytes. We could also have tabulated and stored representatives for each class of reducible form of absolute discriminant up to 10^{10}, but chose not to since our approach to solving equation (31) does not require them.

6.1. **Cases without irreducible forms.** We begin by noting an obvious corollary to Theorem 1 that, in many cases, makes it a relatively routine matter to determine all elliptic curves of a given conductor, provided we can show the nonexistence of certain corresponding cubic forms.

Corollary 2. *Let N be a squarefree positive integer with $\gcd(N, 6) = 1$ and suppose that there do not exist irreducible binary cubic forms in $\mathbb{Z}[x, y]$ of discriminant $\pm 4N_1$, for each positive integer $N_1 \mid N$. Then every elliptic curve over $\mathbb{Q}$ of conductor N_1, for each $N_1 \mid N$, has nontrivial rational 2-torsion.*

We will apply this result to a pair of examples (chosen somewhat arbitrarily). Currently, such an approach is feasible for forms of absolute discriminant (and hence potentially conductors) up to roughly 10^{15}. We observe that, among the positive integers $N < 10^8$ satisfying

$$\nu_2(N) \leq 8, \quad \nu_3(N) \leq 5 \quad \text{and} \quad \nu_p(N) \leq 2 \quad \text{for} \quad p > 3,$$

i.e., those for which there might actually exist elliptic curves $E/\mathbb{Q}$ of conductor N, we find that 708639 satisfies the hypotheses of Corollary 2.

It is somewhat harder to modify the statement of Corollary 2 to include reducible forms (with corresponding elliptic curves having nontrivial rational 2-torsion). One of the difficulties one encounters is that there actually do exist reducible forms of, by way of example, discriminant $4p$ for every $p \equiv 1 \pmod 8$; writing $p = 8k + 1$, for instance, the form

$$F(x, y) = 2x^2y + xy^2 - ky^3$$

has this property.

6.1.1. *Conductor* $2655632887 = 31 \cdot 9007 \cdot 9511$. In the notation of Theorem 1, we have $\alpha = \beta = 0$ and hence $\alpha_0 = 2$ and $\beta_0 = 0$, so that, in order for there to be an elliptic curve with trivial rational 2-torsion and this conductor, we require the existence of an irreducible cubic form of discriminant $4N_1$ where $N_1 \mid 31 \cdot 9007 \cdot 9511$, i.e., discriminant $\pm 4 \cdot 31^{\delta_1} \cdot 9007^{\delta_2} \cdot 9511^{\delta_3}$ for $\delta_i \in \{0, 1\}$. We check that there are no such forms, directly from our table of forms, except for the possibility of $D_F = \pm 4 \cdot 31 \cdot 9007 \cdot 9511$, which exceeds 10^{10} in absolute value. For these latter possibilities, we argue as in Section 5.3 to show that no such forms exist. We may thus appeal to Corollary 2.

For the possible cases with rational 2-torsion, we solve $X + Y = Z^2$ with X and Y S-units for $S = \{2, 31, 9007, 9511\}$. The solutions to this equation with $X \geq Y$,

$Z > 0$, and $\gcd(X, Y)$ squarefree are precisely those with

$$(X, Y) = (2, -1), (2, 2), (8, 1), (32, -31), (62, 2), (256, -31), (961, 128), (992, -31), (3968, 1), (76088, -9007), (294841, 8) \text{ and } (492032, -9007).$$

A short calculation confirms that each elliptic curve arising from these solutions via quadratic twist has bad reduction at the prime 2 (and, in particular, cannot have conductor 2655632887). There are thus no elliptic curves over $\mathbb{Q}$ with conductor 2655632887. Observe that these calculations in fact ensure that there do not exist elliptic curves over $\mathbb{Q}$ with conductor dividing 2655632887.

Full computational details are available at

`http://www.nt.math.ubc.ca/BeGhRe/Examples/2655632887-data`.

We should observe that it is much more challenging computationally to try to extend this argument to tabulate curves E with good reduction outside $S = \{31, 9007, 9511\}$. To do this, we would have to first determine whether or not there exist irreducible cubic forms of discriminant, say, $D_F = \pm 4 \cdot 31^2 \cdot 9007^2 \cdot 9511^2 > 2.8 \times 10^{19}$. This appears to be at or beyond current computational limits.

6.1.2. *Conductor* $3305354359 = 41 \cdot 409 \cdot 439 \cdot 449$. For there to exist an elliptic curve with trivial rational 2-torsion and conductor 3305354359, we require the existence of an irreducible cubic form of discriminant $\pm 4 \cdot 41^{\delta_1} \cdot 409^{\delta_2} \cdot 439^{\delta_3} \cdot 449^{\delta_4}$, with $\delta_i \in \{0, 1\}$. We check that, again, there are no such forms (once more employing a short auxiliary computation in the case $D_F = \pm 4 \cdot 41 \cdot 409 \cdot 439 \cdot 449$). If we solve $X + Y = Z^2$ with X and Y S-units for $S = \{2, 41, 409, 439, 449\}$, we find that the solutions to this equation with $X \geq Y$, $Z > 0$ and $\gcd(X, Y)$ squarefree are precisely:

$$\begin{aligned}(X, Y) = {} & (2, -1), (2, 2), (8, 1), (41, -16), (41, -32), (41, 8), (82, -1), (128, 41), \\ & (409, -328), (409, 32), (439, 2), (449, -328), (449, -8), (512, 449), \\ & (818, 82), (898, 2), (3272, 449), (3362, 2), (7184, 41), (16769, -128), \\ & (16769, -14368), (18409, -16384), (33538, -18409), (36818, 818), \\ & (41984, 41), (68921, -57472), (183641, -1312), (183641, -56192), \\ & (183641, 41984), (359102, 898), (403202, -33538), (403202, -359102), \\ & (403202, 17999), (737959, 183641), (754769, -6544), (6858521, -919552), \\ & (8265641, -16), \text{ and } (7095601778, -5610270178).\end{aligned}$$

Once again, a short calculation confirms that each elliptic curve arising from these solutions via twists has even conductor. There are thus no elliptic curves over $\mathbb{Q}$ with conductor 3305354359.

Full computational details are available at

`http://www.nt.math.ubc.ca/BeGhRe/Examples/3305354359-data`.

6.2. **Cases with fixed conductor (and corresponding irreducible forms).**

6.2.1. *Conductor* $399993 = 3 \cdot 11 \cdot 17 \cdot 23 \cdot 31$. We next choose an example where full data is already available for comparison in the LMFDB [38]. In particular, there are precisely 10 isogeny classes of curves of this conductor (labelled $399993a$ to $399993j$ in the LMFDB), containing a total of 21 isomorphism classes. Of these, 7 isogeny classes (and 18 isomorphism classes) have nontrivial rational 2-torsion.

According to Theorem 1, the curves arise from consideration of cubic forms of discriminant discriminant $\pm 4K$, where $K \mid 3 \cdot 11 \cdot 17 \cdot 23 \cdot 31$. The (reduced) irreducible cubic forms $F(u,v)$ of these discriminants are as follows, where $F(u,v) = \omega_0 u^3 + \omega_1 u^2 v + \omega_2 u v^2 + \omega_3 v^3$:

$(\omega_0,\omega_1,\omega_2,\omega_3)$	D_F	$(\omega_0,\omega_1,\omega_2,\omega_3)$	D_F
$(1,1,1,3)$	$-4\cdot 3\cdot 17$	$(2,4,-6,-3)$	$4\cdot 3\cdot 17\cdot 23$
$(1,2,2,2)$	$-4\cdot 11$	$(2,5,2,6)$	$-4\cdot 3\cdot 17\cdot 23$
$(1,2,2,6)$	$-4\cdot 11\cdot 17$	$(3,3,-8,-2)$	$4\cdot 3\cdot 23\cdot 31$
$(1,4,-16,-2)$	$4\cdot 11\cdot 17\cdot 31$	$(3,3,44,66)$	$-4\cdot 3\cdot 11\cdot 17\cdot 23\cdot 31$
$(1,8,-2,42)$	$-4\cdot 3\cdot 17\cdot 23\cdot 31$	$(3,4,10,14)$	$-4\cdot 11\cdot 23\cdot 31$
$(1,11,-12,-6)$	$4\cdot 3\cdot 11\cdot 17\cdot 31$	$(3,7,5,7)$	$-4\cdot 3\cdot 23\cdot 31$
$(2,0,7,1)$	$-4\cdot 23\cdot 31$	$(4,17,10,28)$	$-4\cdot 11\cdot 17\cdot 23\cdot 31$
$(2,1,14,-2)$	$-4\cdot 11\cdot 17\cdot 31$		

In each case, we are thus led to solve the Thue-Mahler equation

$$F(u,v) = 2^{3\delta} 3^{\beta_1} 11^{\kappa_{11}} 17^{\kappa_{17}} 23^{\kappa_{23}} 31^{\kappa_{31}}, \tag{32}$$

where $\gcd(u,v) = 1$, $\delta \in \{0,1\}$ and β_1, κ_{11}, κ_{17}, κ_{23} and κ_{31} are arbitrary non-negative integers. Applying (13), in order to find a curve of conductor 399993, we require additionally that, for a corresponding solution to (32),

$$F(u,v)\, D_F \equiv 0 \pmod{3\cdot 11\cdot 17\cdot 23\cdot 31}. \tag{33}$$

We readily check that the congruence $F(u,v) \equiv 0 \pmod p$ has only the solution $u \equiv v \equiv 0 \pmod p$ for the following forms F and primes p (whereby (33) cannot be satisfied by coprime integers u and v for these forms):

$(\omega_0,\omega_1,\omega_2,\omega_3)$	p	$(\omega_0,\omega_1,\omega_2,\omega_3)$	p
$(1,1,1,3)$	$11, 23$	$(2,0,7,1)$	$3, 17$
$(1,2,2,2)$	$3, 23, 31$	$(2,5,2,6)$	$11, 31$
$(1,4,-16,-2)$	$3, 23$	$(3,3,-8,-2)$	11
$(1,8,-2,42)$	11	$(4,17,10,28)$	3
$(1,11,-12,-6)$	23		

For the remaining 6 forms under consideration, we appeal to UBC-TM. The only solutions we find satisfying (33) are as follows:

$(\omega_0,\omega_1,\omega_2,\omega_3)$	(u,v)
$(1,2,2,6)$	$(-1851,892), (14133,-3790)$
$(2,1,14,-2)$	$(13,-5), (-29,-923)$
$(2,4,-6,-3)$	$(10,-3), (64,49), (-95,199), (-3395,1189),$ $(3677,-1069), (5158,4045), (-23546,57259), (-77755,30999)$
$(3,3,44,66)$	$(1,0), (1,2), (-3,4), (3,-2), (-11,9), (25,-3),$ $(231,2), (-317,240), (489,61), (1263,-878), (6853,-4119)$
$(3,7,5,7)$	$(1,12), (-29,26), (78,1), (423,-160)$
$(3,4,10,14)$	$(-41,84), (95,-69), (307,90)$

From these, we compute the conductors of $E_{\mathcal{D}}$ in (8), where $\mathcal{D} \in \{1,2\}$, together with their twists by -1. The only curves with conductor 399993 arise from the form F with $(\omega_0,\omega_1,\omega_2,\omega_3) = (2,4,-6,-3)$ and the solutions

$$(u,v) \in \{(10,-3), (5158,4045), (-23546,57259)\}.$$

In each case, $\mathcal{D} = 2$. The solution $(u, v) = (10, -3)$ corresponds to, in the notation of the LMFBD, curve 399993.j1, $(u, v) = (5158, 4045)$ to 399993.i1, and $(u, v) = (-23546, 57259)$ to 399993.h1. Note that every form and solution we consider leads to elliptic curves with good reduction outside $\{2, 3, 11, 17, 23, 31\}$, just not necessarily of conductor 399993. By way of example, if $(\omega_0, \omega_1, \omega_2, \omega_3) = (2, 4, -6, -3)$ and $(u, v) = (-77755, 30999)$, we find curves with minimal quadratic twists of conductor

$$2^5 \cdot 3 \cdot 11 \cdot 17 \cdot 23 \cdot 31 = 2^5 \cdot 399993.$$

To determine the curves of conductor 399993 with nontrivial rational 2-torsion, we are led to solve the equation $X + Y = Z^2$ in S-units X and Y, and integers Z, where $S = \{2, 3, 11, 17, 23, 31\}$. We employ Magma code available at

`http://nt.math.ubc.ca/BeGhRe/Code/UBC-TMCode`

to find precisely 2858 solutions with $X \geq |Y|$ and $\gcd(X, Y)$ squarefree (this computation took slightly less than 2 hours). Of these, 1397 have $Z > 0$, with Z largest for the solution corresponding to the identity

$$48539191572432 - 40649300451407 = 2^4 \cdot 3^4 \cdot 11 \cdot 23^7 - 17^5 \cdot 31^5 = 2808895^2.$$

As in subsection 5.2, we attach to each solution a pair of elliptic curves $E_1(X, Y)$ and $E_2(X, Y)$. Of these, the only twists we find to have conductor 399993 are the quadratic twists by t of $E_i(X, Y)$ given in the following table. Note that there is some duplication—the curve labelled 399993.f2 in the LMFDB, for example, arises from three distinct solutions to $X + Y = Z^2$:

X	Y	E_i	t	LMFDB	X	Y	E_i	t	LMFDB
16192	−4743	E_1	−1	399993.$g2$	534336	−506447	E_2	2	399993.$e1$
16192	−4743	E_2	2	399993.$g1$	1311552	−527	E_1	1	399993.$a2$
23529	18496	E_1	−2	399993.$f2$	1311552	−527	E_2	−2	399993.$a1$
23529	18496	E_2	1	399993.$f3$	1414017	−1045568	E_1	2	399993.$b2$
116281	−75072	E_1	2	399993.$f4$	1414017	−1045568	E_2	−1	399993.$b1$
116281	−75072	E_2	−1	399993.$f2$	6305121	3027904	E_1	2	399993.$c1$
371008	4761	E_1	1	399993.$f2$	6305121	3027904	E_2	−1	399993.$c2$
371008	4761	E_2	−2	399993.$f1$	6988113	18496	E_1	2	399993.$c2$
519777	−131648	E_1	2	399993.$d2$	6988113	18496	E_2	−1	399993.$c3$
519777	−131648	E_2	−1	399993.$d1$	7745089	−2731968	E_1	2	399993.$c4$
534336	−506447	E_1	−1	399993.$e2$	7745089	−2731968	E_2	−1	399993.$c2$

Full computational details are available at

`http://www.nt.math.ubc.ca/BeGhRe/Examples/399993-data`.

6.2.2. *Conductor* $10^6 - 1$. We next treat a slightly larger conductor, which is not available in the LMFDB currently (but probably within computational range). We have

$$10^6 - 1 = 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37.$$

From Theorem 1, we thus need to consider binary cubic forms $F(u, v) = \omega_0 u^3 + \omega_1 u^2 v + \omega_2 u v^2 + \omega_3 v^3$ of discriminant $D_F = \pm 108 N_1$, where $N_1 \mid 7 \cdot 11 \cdot 13 \cdot 37$ and

$\omega_1 \equiv \omega_2 \equiv 0 \pmod 3$. The irreducible forms of this shape are as follows:

$(\omega_0, \omega_1, \omega_2, \omega_3)$	D_F	p	$(\omega_0, \omega_1, \omega_2, \omega_3)$	D_F	p
$(1, 0, -6, -2)$	$108 \cdot 7$	37	$(2, 3, -78, -26)$	$108 \cdot 7 \cdot 11 \cdot 13 \cdot 37$	none
$(1, 0, 21, 16)$	$-108 \cdot 11 \cdot 37$	7, 13	$(2, 3, 6, 3)$	$-108 \cdot 7$	11, 37
$(1, 0, 30, 2)$	$-108 \cdot 7 \cdot 11 \cdot 13$	none	$(2, 3, 6, 8)$	$-108 \cdot 37$	7
$(1, 3, 3, 3)$	-108	7, 13, 37	$(2, 6, -12, 1)$	$108 \cdot 11 \cdot 13$	7
$(1, 3, 6, 16)$	$-108 \cdot 37$	7	$(2, 6, 21, 88)$	$-108 \cdot 11 \cdot 13 \cdot 37$	none
$(1, 3, 12, 26)$	$-108 \cdot 7 \cdot 13$	none	$(2, 12, 0, 13)$	$-108 \cdot 7 \cdot 11 \cdot 13$	none
$(1, 3, 33, 117)$	$-108 \cdot 7 \cdot 11 \cdot 37$	none	$(2, 21, -6, 80)$	$-108 \cdot 7 \cdot 11 \cdot 13 \cdot 37$	none
$(1, 6, -36, -34)$	$108 \cdot 7 \cdot 13 \cdot 37$	11	$(3, 3, 18, 20)$	$-108 \cdot 7 \cdot 11 \cdot 13$	none
$(1, 6, 3, 6)$	$-108 \cdot 37$	7	$(4, 6, 15, 14)$	$-108 \cdot 13 \cdot 37$	11
$(1, 6, 9, 26)$	$-108 \cdot 11 \cdot 13$	none	$(5, 6, 27, 14)$	$-108 \cdot 7 \cdot 11 \cdot 37$	none
$(1, 9, 0, 74)$	$-108 \cdot 7 \cdot 13 \cdot 37$	none	$(5, 9, 3, 21)$	$-108 \cdot 7 \cdot 11 \cdot 37$	none
$(1, 12, 12, 14)$	$-108 \cdot 13 \cdot 37$	11	$(7, 0, 12, 14)$	$-108 \cdot 7 \cdot 11 \cdot 37$	none
$(2, 0, -18, -5)$	$108 \cdot 11 \cdot 37$	13	$(10, 3, 42, -16)$	$-108 \cdot 7 \cdot 11 \cdot 13 \cdot 37$	none
$(2, 0, 3, 3)$	$-108 \cdot 11$	7, 37	$(10, 6, 12, 3)$	$-108 \cdot 13 \cdot 37$	none
$(2, 0, 15, 3)$	$-108 \cdot 7 \cdot 37$	11, 13	$(11, 6, 12, 6)$	$-108 \cdot 7 \cdot 11 \cdot 13$	none
$(2, 0, 18, 7)$	$-108 \cdot 13 \cdot 37$	11	$(21, 12, 27, 20)$	$-108 \cdot 7 \cdot 11 \cdot 13 \cdot 37$	none

Here, we list primes p for which a local obstruction exists modulo p to finding coprime integers u and v satisfying (13). It is worth noting at this point that the restriction to forms with $\omega_1 \equiv \omega_2 \equiv 0 \pmod 3$ that follows from the fact that we are considering a conductor divisible by 3^3 is a helpful one. There certainly can and do exist irreducible forms F with $108 \mid D_F$ that fail to satisfy $\omega_1 \equiv \omega_2 \equiv 0 \pmod 3$.

We are thus left to treat 17 Thue-Mahler equations which we solve using UBC-TM; see

`http://www.nt.math.ubc.ca/BeGhRe/Examples/999999-data`

for computational details. From (13), we require that

$$D_F F(u, v) \equiv 0 \pmod{7 \cdot 11 \cdot 13 \cdot 37};$$

the only solutions we find satisfying this constraint are as follows:

$(\omega_0, \omega_1, \omega_2, \omega_3)$	(u, v)
$(1, 0, 30, 2)$	$(-1, 21), (1, 16), (27, 25)$
$(1, 3, 33, 117)$	$(26, -7)$
$(1, 9, 0, 74)$	$(-19, 2)$
$(2, 3, -78, -26)$	$(-1, 3), (-3, 2), (-5, -1), (9, -1), (13, 2), (-17, -58), (-39, -61),$ $(-57, -10), (-59, 9), (65, -6), (79, -330), (159, -23)$
$(2, 6, 21, 88)$	$(3, 1), (165, -43)$
$(2, 12, 0, 13)$	$(-1, 9), (18, 23)$
$(2, 21, -6, 80)$	$(1, -10), (2, 1), (4, -3), (4, -1), (17, 1),$ $(19, -5), (21, -2), (138, -11), (1356, -127)$
$(3, 3, 18, 20)$	$(9, 13), (97, -12)$
$(5, 6, 27, 14)$	$(14, 1), (19, 6), (-21, 44)$
$(5, 9, 3, 21)$	$(-1, 2), (6, 1), (8, -3), (-649, 284), (1077, -464)$
$(7, 0, 12, 14)$	$(-1, 5), (-7, 9), (301, -62), (-459, 553)$
$(10, 3, 42, -16)$	$(1, 1), (1, 2), (2, -1), (3, 1), (4, -17), (20, 19), (-22, -69), (127, 339)$
$(10, 6, 12, 3)$	$(2, -1), (5, -13), (-12, 83), (-24, 89), (81, -107), (125, -437)$
$(11, 6, 12, 6)$	$(-1, 22), (47, -72), (223, -429)$
$(21, 12, 27, 20)$	$(1, -3), (1, 0), (1, 5), (4, -9), (4, 3), (9, -29),$ $(19, -15), (29, -40), (316, -455), (551, -805)$

The only ones of these for which we find an $E_{\mathcal{D}}$ in (8) of conductor 999999 are as follows, where $E_{\mathcal{D}}$ is isomorphic over $\mathbb{Q}$ to a curve with model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

$(\omega_0, \omega_1, \omega_2, \omega_3)$	(u, v)	$\mathcal{D}$	a_1	a_2	a_3	a_4	a_6
$(1, 0, 30, 2)$	$(27, 25)$	6	0	0	1	-40395	5402579
$(1, 0, 30, 2)$	$(27, 25)$	-2	0	0	1	-363555	-145869640
$(5, 6, 27, 14)$	$(14, 1)$	1	1	-1	0	14700	55223
$(5, 6, 27, 14)$	$(14, 1)$	-3	1	-1	1	1633	-2590
$(5, 9, 3, 21)$	$(-1, 2)$	6	0	0	1	30	2254
$(5, 9, 3, 21)$	$(-1, 2)$	-2	0	0	1	270	-60865
$(10, 6, 12, 3)$	$(125, -437)$	2	0	0	1	-17205345	-27554570341
$(10, 6, 12, 3)$	$(125, -437)$	-6	0	0	1	-1911705	1020539642
$(21, 12, 27, 20)$	$(4, 3)$	-1	1	-1	0	12432	-164125
$(21, 12, 27, 20)$	$(4, 3)$	3	1	-1	1	1381	5618

Each of these listed curves has trivial rational 2-torsion. To search for curves of conductor 999999 with nontrivial rational 2-torsion, we solve the equation $X+Y = Z^2$ in S-units X and Y, and integers Z, where $S = \{2, 3, 7, 11, 13, 37\}$. We find that there are precisely 4336 solutions with $X \geq |Y|$ and $\gcd(X, Y)$ squarefree. Of these, 2136 have $Z > 0$, with Z largest for the solution corresponding to the identity

$$103934571636753 - 68209863326528 = 3^{15} \cdot 11 \cdot 13 \cdot 37^3 - 2^6 \cdot 7^{13} \cdot 11 = 5977015^2.$$

Once again, we attach to each solution a pair of elliptic curves $E_1(X, Y)$ and $E_2(X, Y)$. We find 505270 isomorphism classes of $E/\mathbb{Q}$ with good reduction outside of $\{2, 3, 7, 11, 13, 37\}$ and nontrivial rational 2-torsion. None of them have conductor 999999, whereby we conclude that there are precisely 10 isomorphism classes of elliptic curves over $\mathbb{Q}$ with conductor $10^6 - 1$. Checking that these curves each have distinct traces of Frobenius a_{47} shows that they are nonisogenous.

6.2.3. *Conductor* $10^9 - 1$. This example is chosen to be somewhat beyond the current scope of the LMFDB. We have

$$10^9 - 1 = 3^4 \cdot 37 \cdot 333667$$

and so, applying Theorem 1, we are led to consider binary cubic forms of discriminant $\pm 4 \cdot 3^4 \cdot 37^{\delta_1} \cdot 333667^{\delta_2}$, where $\delta_i \in \{0, 1\}$. These include imprimitive forms with the property that each of its coefficients ω_i is divisible by 3. For such forms, from Theorem 1, we necessarily have $\beta_1 \in \{0, 1\}$ and hence $\beta_1 = 1$. Dividing through by 3, we may thus restrict our attention to primitive forms of discriminant $\pm 4 \cdot 3^{\kappa} \cdot 37^{\delta_1} \cdot 333667^{\delta_2}$, where $\delta_i \in \{0, 1\}$ and $\kappa \in \{0, 4\}$. For the irreducible forms, we have, by slight abuse of notation (since, for the F listed here with $D_F \not\equiv 0 \pmod 3$),

the form whose existence is guaranteed by Theorem 1 is actually $3F$), the following.

$(\omega_0,\omega_1,\omega_2,\omega_3)$	D_F	p	$(\omega_0,\omega_1,\omega_2,\omega_3)$	D_F	p
$(1,1,-3,-1)$	$4\cdot 37$	333667	$(5,14,19,54)$	$-4\cdot 333667$	37
$(1,4,52,250)$	$-4\cdot 333667$	37	$(6,18,168,323)$	$-4\cdot 3^4\cdot 333667$	37
$(1,9,37,279)$	$-4\cdot 333667$	none	$(6,27,42,356)$	$-4\cdot 3^4\cdot 333667$	37
$(1,21,117,2135)$	$-4\cdot 3^4\cdot 333667$	37	$(6,54,-48,115)$	$-4\cdot 3^4\cdot 333667$	37
$(2,0,3,1)$	$-4\cdot 3^4$	37	$(10,18,96,229)$	$-4\cdot 3^4\cdot 333667$	37
$(2,17,-26,-31)$	$4\cdot 333667$	37	$(26,9,102,4)$	$-4\cdot 3^4\cdot 333667$	none
$(4,30,117,665)$	$-4\cdot 3^4\cdot 333667$	37	$(27,7,70,32)$	$-4\cdot 37\cdot 333667$	none
$(4,35,14,216)$	$-4\cdot 37\cdot 333667$	none	$(31,9,87,-25)$	$-4\cdot 3^4\cdot 333667$	none
$(5,6,9,6)$	$-4\cdot 3^4\cdot 37$	none	$(49,51,63,55)$	$-4\cdot 3^4\cdot 333667$	none
$(5,7,19,51)$	$-4\cdot 333667$	37	$(52,55,72,37)$	$-4\cdot 37\cdot 333667$	none

Once again, we list primes p for which a local obstruction exists modulo p to finding coprime integers u and v satisfying (13). There are thus 8 Thue-Mahler equations left to solve. In the (four) cases where $D_F \not\equiv 0 \pmod 3$, these take the shape

$$F(u,v) = 2^{3\delta_1}\cdot 37^{\gamma_1}\cdot 333667^{\gamma_2},$$

where $\delta_1 \in \{0,1\}$, γ_1 and γ_2 are nonnegative integers, and u and v are coprime integers. For the remaining F, the analogous equation is

$$F(u,v) = 2^{3\delta_1}\cdot 3^{\delta_2}\cdot 37^{\gamma_1}\cdot 333667^{\gamma_2},$$

where $\delta_i \in \{0,1\}$, $\gamma_1,\gamma_2 \in \mathbb{Z}^+$ and $u,v \in \mathbb{Z}$ with $\gcd(u,v)=1$. We solve these equations using the UBC-TM Thue-Mahler solver. The only cases where we find that

$$D_F F(u,v) \equiv 0 \pmod{37\cdot 333667}$$

occur for $(\omega_0,\omega_1,\omega_2,\omega_3) = (4,35,14,216)$ and $(u,v) = (-8,1)$ or $(u,v) = (-2,1)$, for $(\omega_0,\omega_1,\omega_2,\omega_3) = (27,7,70,32)$ and $(u,v) = (1,-2)$ or $(2,-1)$, and for $(\omega_0,\omega_1,\omega_2,\omega_3) = (52,55,72,37)$ and $(u,v) = (0,1)$ or $(-3,5)$. In each case, all resulting twists have bad reduction at 2 (and hence cannot have conductor 10^9-1).

To search for curves with nontrivial rational 2-torsion and conductor 10^9-1, we solve the equation $X+Y=Z^2$ in S-units X and Y, and integers Z, where $S=\{2,3,37,333667\}$. There are precisely 98 solutions with $X \geq |Y|$ and $\gcd(X,Y)$ squarefree. Of these, 41 have $Z>0$, with Z largest for the solution coming from the identity

$$27027027 - 101306 = 3^4\cdot 333667 - 2\cdot 37^3 = 5189^2.$$

These correspond via twists to elliptic curves of conductor as large as $2^8\cdot 3^2\cdot 37^2\cdot 333667^2$, but none of conductor 10^9-1. There thus exist no curves $E/\mathbb{Q}$ of conductor 10^9-1.

Full computational details are available at

`http://www.nt.math.ubc.ca/BeGhRe/Examples/999999999-data`.

6.3. **Curves with good reduction outside $\{2,3,23\}$: An example of Koutsianis and of von Kanel and Matchke.** This case was worked out by Koutsianis [37] (and also by von Kanel and Matschke [36], who actually computed $E/\mathbb{Q}$ with good reduction outside $\{2,3,p\}$ for all prime $p \leq 163$), by rather different methods from those employed here. We include it here to provide an example where we determine all $E/\mathbb{Q}$ with good reduction outside a specific set S, which is of somewhat

manageable size in terms of the set of cubic forms encountered. Our data agrees with that of [36] and [37].

To begin, we observe that the elliptic curves with good reduction outside $\{2, 3, 23\}$ and j-invariant 0 are precisely those with models of the shape

$$E \quad : \quad Y^2 = X^3 \pm 2^a 3^b 23^c, \quad \text{where} \quad 0 \le a, b, c \le 5.$$

Appealing to (14), we next look through our precomputed list to find all the irreducible primitive cubic forms of discriminant $\pm 2^\alpha 3^\beta 23^\gamma$, where

$$\alpha \in \{0, 2, 3, 4\}, \quad \beta \in \{0, 1, 3, 4, 5\}, \quad \text{and} \quad \gamma \in \{0, 1, 2\}.$$

The imprimitive forms we need consider correspond to primitive forms F with either $\nu_2(D_F) = 0$ or $\nu_3(D_F) \in \{0, 1\}$. We find precisely 95 irreducible, primitive cubic forms of the desired discriminants.

$(\omega_0, \omega_1, \omega_2, \omega_3)$	D_F	$(\omega_0, \omega_1, \omega_2, \omega_3)$	D_F	$(\omega_0, \omega_1, \omega_2, \omega_3)$	D_F
$(1, 0, -18, -6)$	$2^2 \cdot 3^5 \cdot 23$	$(2, 0, 3, 4)$	$-2^3 \cdot 3^5$	$(4, 9, 24, 29)$	$-2^2 \cdot 3^4 \cdot 23^2$
$(1, 0, -3, -1)$	3^4	$(2, 3, 6, 4)$	$-2^2 \cdot 3^5$	$(4, 12, 12, 27)$	$-2^4 \cdot 3^3 \cdot 23^2$
$(1, 0, 3, 2)$	$-2^3 \cdot 3^3$	$(2, 3, 12, 8)$	$-2^4 \cdot 3^3 \cdot 23$	$(4, 12, 12, 73)$	$-2^4 \cdot 3^5 \cdot 23^2$
$(1, 0, 6, 2)$	$-2^2 \cdot 3^5$	$(2, 3, 36, 29)$	$-2^3 \cdot 3^4 \cdot 23^2$	$(4, 18, 9, 24)$	$-2^2 \cdot 3^5 \cdot 23^2$
$(1, 0, 6, 4)$	$-2^4 \cdot 3^4$	$(2, 3, 36, 98)$	$-2^3 \cdot 3^5 \cdot 23^2$	$(4, 18, 27, 48)$	$-2^2 \cdot 3^5 \cdot 23^2$
$(1, 0, 9, 6)$	$-2^4 \cdot 3^5$	$(2, 5, 8, 15)$	$-2^3 \cdot 3 \cdot 23^2$	$(5, 6, 7, 4)$	$-2^3 \cdot 23^2$
$(1, 0, 33, 32)$	$-2^2 \cdot 3^4 \cdot 23^2$	$(2, 6, -12, -1)$	$2^2 \cdot 3^5 \cdot 23$	$(5, 6, 15, 8)$	$-2^3 \cdot 3^5 \cdot 23$
$(1, 1, 2, 1)$	-23	$(2, 6, 6, 5)$	$-2^2 \cdot 3^5$	$(5, 9, 12, 10)$	$-2^2 \cdot 3^5 \cdot 23$
$(1, 1, 8, 6)$	$-2^2 \cdot 23^2$	$(2, 6, 6, 25)$	$-2^2 \cdot 3^3 \cdot 23^2$	$(5, 12, 18, 20)$	$-2^4 \cdot 3^5 \cdot 23$
$(1, 3, -9, -4)$	$3^5 \cdot 23$	$(2, 6, 27, 117)$	$-2^3 \cdot 3^5 \cdot 23^2$	$(5, 18, 30, 46)$	$-2^2 \cdot 3^5 \cdot 23^2$
$(1, 3, -6, -4)$	$2^2 \cdot 3^3 \cdot 23$	$(2, 9, -6, -4)$	$2^2 \cdot 3^5 \cdot 23$	$(5, 24, -3, 26)$	$-2^4 \cdot 3^5 \cdot 23^2$
$(1, 3, -3, -2)$	$3^3 \cdot 23$	$(2, 9, 0, -4)$	$2^4 \cdot 3^3 \cdot 23$	$(6, 3, 12, -7)$	$-2^3 \cdot 3^3 \cdot 23^2$
$(1, 3, -6, -2)$	$2^3 \cdot 3^5$	$(2, 9, 48, 185)$	$-2^4 \cdot 3^5 \cdot 23^2$	$(6, 3, 12, 16)$	$-2^4 \cdot 3^3 \cdot 23^2$
$(1, 3, 3, 3)$	$-2^2 \cdot 3^3$	$(2, 12, 24, 85)$	$-2^2 \cdot 3^5 \cdot 23^2$	$(6, 6, 9, 13)$	$-2^3 \cdot 3^3 \cdot 23^2$
$(1, 3, 3, 5)$	$-2^4 \cdot 3^3$	$(2, 18, -15, 31)$	$-2^3 \cdot 3^5 \cdot 23^2$	$(6, 9, 12, 23)$	$-2^3 \cdot 3^4 \cdot 23^2$
$(1, 3, 3, 7)$	$-2^2 \cdot 3^5$	$(3, 0, 3, 2)$	$-2^4 \cdot 3^4$	$(6, 18, 18, 29)$	$-2^2 \cdot 3^5 \cdot 23^2$
$(1, 3, 3, 13)$	$-2^4 \cdot 3^5$	$(3, 4, 12, 12)$	$-2^4 \cdot 3 \cdot 23^2$	$(7, 6, 9, 4)$	$-2^3 \cdot 3^4 \cdot 23$
$(1, 3, 18, 50)$	$-2^3 \cdot 3^5 \cdot 23$	$(3, 6, 4, 6)$	$-2^2 \cdot 3 \cdot 23^2$	$(7, 15, 3, 17)$	$-2^2 \cdot 3^5 \cdot 23^2$
$(1, 6, -24, -4)$	$2^4 \cdot 3^5 \cdot 23$	$(3, 6, 9, 8)$	$-2^3 \cdot 3^3 \cdot 23$	$(8, 9, 12, 13)$	$-2^2 \cdot 3^4 \cdot 23^2$
$(1, 6, 3, 32)$	$-2^3 \cdot 3^5 \cdot 23$	$(3, 9, 9, 7)$	$-2^4 \cdot 3^5$	$(8, 15, 18, 21)$	$-2^3 \cdot 3^4 \cdot 23^2$
$(1, 6, 6, 16)$	$-2^4 \cdot 3^3 \cdot 23$	$(3, 9, 9, 49)$	$-2^2 \cdot 3^5 \cdot 23^2$	$(9, 9, 3, 31)$	$-2^4 \cdot 3^5 \cdot 23^2$
$(1, 6, 12, 54)$	$-2^2 \cdot 3^3 \cdot 23^2$	$(3, 18, 36, 116)$	$-2^4 \cdot 3^5 \cdot 23^2$	$(10, 6, 15, 1)$	$-2^3 \cdot 3^3 \cdot 23^2$
$(1, 6, 12, 100)$	$-2^4 \cdot 3^3 \cdot 23^2$	$(3, 27, 9, 29)$	$-2^4 \cdot 3^5 \cdot 23^2$	$(11, 6, 12, 2)$	$-2^2 \cdot 3^3 \cdot 23^2$
$(1, 9, -12, -16)$	$2^4 \cdot 3^5 \cdot 23$	$(4, 0, -18, -3)$	$2^4 \cdot 3^5 \cdot 23$	$(11, 15, 15, 17)$	$-2^2 \cdot 3^5 \cdot 23^2$
$(1, 9, -9, -3)$	$2^2 \cdot 3^5 \cdot 23$	$(4, 0, 6, 1)$	$-2^4 \cdot 3^5$	$(12, 9, 36, 16)$	$-2^4 \cdot 3^5 \cdot 23^2$
$(1, 9, 27, 165)$	$-2^2 \cdot 3^5 \cdot 23^2$	$(4, 2, 8, 3)$	$-2^4 \cdot 23^2$	$(12, 36, 36, 35)$	$-2^4 \cdot 3^5 \cdot 23^2$
$(1, 9, 27, 303)$	$-2^4 \cdot 3^5 \cdot 23^2$	$(4, 3, 6, 2)$	$-2^2 \cdot 3^3 \cdot 23$	$(13, 9, 18, 12)$	$-2^2 \cdot 3^5 \cdot 23^2$
$(1, 12, 9, 18)$	$-2^4 \cdot 3^5 \cdot 23$	$(4, 3, 12, 10)$	$-2^3 \cdot 3^5 \cdot 23$	$(13, 15, 27, 7)$	$-2^2 \cdot 3^5 \cdot 23^2$
$(1, 12, 12, 44)$	$-2^4 \cdot 3^3 \cdot 23^2$	$(4, 3, 18, 13)$	$-2^3 \cdot 3^3 \cdot 23^2$	$(21, 9, 27, 11)$	$-2^4 \cdot 3^5 \cdot 23^2$
$(1, 15, 3, -7)$	$2^4 \cdot 3^5 \cdot 23$	$(4, 3, 18, 36)$	$-2^2 \cdot 3^5 \cdot 23^2$	$(23, 30, 36, 20)$	$-2^4 \cdot 3^5 \cdot 23^2$
$(2, 0, 3, 1)$	$-2^2 \cdot 3^4$	$(4, 4, 9, 1)$	$-2^4 \cdot 23^2$	$(24, 27, 36, 16)$	$-2^4 \cdot 3^5 \cdot 23^2$
$(2, 0, 3, 2)$	$-2^3 \cdot 3^4$	$(4, 6, 3, 12)$	$-2^2 \cdot 3^3 \cdot 23^2$		

In each case, we solve the corresponding Thue-Mahler equation specified by Theorem 1. For example, if $D_F = \pm 2^4 \cdot 3^t \cdot 23^2$, with $t \ge 3$, then we actually need only solve the (eight) Thue equations of the shape

$$F(u, v) = 2^{\delta_1} 3^{\delta_2} 23^{\delta_3}, \quad \text{where} \quad \delta_i \in \{0, 1\}.$$

For all other discriminants, we must treat "genuine" Thue-Mahler equations (where at least one of the exponents on the right-hand side of equation (7) is, a priori, unconstrained). Details of this computation are available at

`http://www.nt.math.ubc.ca/BeGhRe/Examples/2-3-23-data`.

In total, we found precisely 730 solutions to these equations, leading, after twisting, to 3856 isomorphism classes of $E/\mathbb{Q}$ with good reduction outside $\{2, 3, 23\}$ and trivial rational 2-torsion.

Once again, to find the curves with nontrivial rational 2-torsion, we solved $X + Y = Z^2$ in S-units X and Y, and integers Z, where $S = \{2, 3, 23\}$. There are precisely 118 solutions with $X \geq |Y|$ and $\gcd(X, Y)$ squarefree (this computation took less than 1 hour). Of these, 55 have $Z > 0$, with Z largest for the solution coming from the identity

$$89424 - 23 = 2^4 \cdot 3^5 \cdot 23 - 23 = 299^2.$$

These correspond via twists to elliptic curves of conductor as large as $2^8 \cdot 3^2 \cdot 23^2$, a total of 1664 isomorphism classes. Thus, there exist a total of 5520 isomorphism classes (in 3968 isogeny classes) of elliptic curves $E/\mathbb{Q}$ with good reduction outside $\{2, 3, 23\}$. Note that $432 = 2 \times 6^3$ of these have $j_E = 0$.

6.4. **Curves with good reduction outside $\{2, 3, 5, 7, 11\}$: An example of von Kanel and Matschke.** This is the largest computation carried out along these lines by von Kanel and Matschke [36] (and also a very substantial computation via our approach, taking many thousand machine hours on 80 cores).

As in the preceding example, note that the curves with models of the shape

$$E \ : \ Y^2 = X^3 \pm 2^a 3^b 5^c 7^d 11^e, \ \ 0 \leq a, b, c, d, e \leq 5$$

are precisely the $E/\mathbb{Q}$ with good reduction outside $\{2, 3, 5, 7, 11\}$ and j-invariant 0. We next proceed by searching our precomputed list for all irreducible primitive cubic forms of discriminant $2^\alpha 3^\beta M$, where

$$\alpha \in \{0, 2, 3, 4\}, \ \ \beta \in \{0, 1, 3, 4, 5\}, \quad \text{and} \quad M \mid 5^2 \cdot 7^2 \cdot 11^2.$$

The imprimitive forms we need consider again correspond to primitive forms F with either $\nu_2(D_F) = 0$ or $\nu_3(D_F) \in \{0, 1\}$. We encounter 1796 irreducible cubic forms, which we tabulate at

`http://www.nt.math.ubc.ca/BeGhRe/Examples/2-3-5-7-11-data`,

where details on the resulting Thue-Mahler computation may also be found. Confirming the results of von Kanel and Matschke [36], we find that there exist a total of 592192 isomorphism classes (in 453632 isogeny classes) of elliptic curves $E/\mathbb{Q}$ with good reduction outside $\{2, 3, 5, 7, 11\}$, including $15552 = 2 \times 6^5$ with $j_E = 0$.

7. Good reduction outside a single prime

For the remainder of this paper, we will focus our attention on the case of elliptic curves with bad reduction at a single prime, i.e., curves of conductor p or p^2, for p prime. In this case, our approach simplifies considerably and rather than being required to solve Thue-Mahler equations, the problem reduces to one of solving *Thue* equations, i.e., equations of the shape $F(x, y) = m$, where F is a form and m is a fixed integer. While, once again, we do not have a detailed computational complexity analysis of either algorithms for solving Thue equations or more general algorithms for solving Thue-Mahler equations, computations to date strongly support the contention that the former is, usually, much, much faster than the latter, particularly if the set of primes S considered for the Thue-Mahler equations is anything other than tiny. Since none of these conductors are divisible by 9, we may always suppose that $j_E \neq 0$. We note that the data we have produced

in these cases totals several terabytes. As a result, we have not yet determined how best to make it publicly available; interested readers should contact the authors for further details.

7.1. **Conductor $N = p$.** Suppose that E is a curve with conductor $N = p$ prime with invariants c_4 and c_6. From Tables 1, 2, and 3, we necessarily have one of

$$\begin{aligned}
&(\nu_2(c_4), \nu_2(c_6)) = (0,0) \text{ or } (\geq 4, 3), \text{ and } \nu_2(\Delta_E) = 0, \quad \text{or} \\
&(\nu_3(c_4), \nu_3(c_6)) = (0,0) \text{ or } (1, \geq 3), \text{ and } \nu_3(\Delta_E) = 0, \quad \text{or} \\
&(\nu_p(c_4), \nu_p(c_6)) = (0,0) \text{ and } \nu_p(\Delta_E) \geq 1.
\end{aligned}$$

From this we see that $\mathcal{D} = 1$ or 2. Theorem 1 then implies that there is a cubic form of discriminant ± 4 or $\pm 4p$, and integers u, v, with

$$F(u,v) = p^{\kappa_p} \text{ or } 8p^{\kappa_p}, \quad c_4 = \mathcal{D}^2 H_F(u,v) \quad \text{and} \quad c_6 = -\frac{1}{2}\mathcal{D}^3 G_F(u,v),$$

for $\mathcal{D} \in \{1,2\}$ and κ_p a nonnegative integer. Note that, while the smallest absolute discriminant for an irreducible cubic form in $\mathbb{Z}[x,y]$ is 23, there do exist reducible cubic forms of discriminants 4 and -4 which we must consider.

Appealing to Théorème 2 of Mestre and Oesterlé [43] (and using [10]), we can actually restrict the choices for n dramatically. In fact, we have 3 possibilities: either $p \in \{11, 17, 19, 37\}$, or $p = t^2 + 64$ for some integer t, or, in all other cases, $\Delta_E = \pm p$. There are precisely 14 isomorphism classes of $E/\mathbb{Q}$ with conductor in $\{11, 17, 19, 37\}$; one may consult Cremona [15] for details. If we can write $p = t^2 + 64$ for an integer t (which we may, without loss of generality, assume to satisfy $t \equiv 1 \pmod 4$), then the (2-isogenous) curves defined by

$$y^2 + xy = x^3 + \frac{t-1}{4} \cdot x^2 - x$$

and

$$y^2 + xy = x^3 + \frac{t-1}{4} \cdot x^2 + 4x + t$$

have rational points of order 2 given by $(x,y) = (0,0)$ and $(x,y) = (-t/4, t/8)$, respectively, and discriminants t^2+64 and $-(t^2+64)^2$, respectively. In the final case (in which $\Delta_E = \pm p$), we have (using the notation of Section 3 and, in particular, appealing to (10) which, in this case yields the equation $1 = \nu_p(\Delta_E) = \nu_p(D_F) + 2\kappa_p$)

$$\alpha_0 = 2, \ \alpha_1 \in \{0,3\}, \ \beta_0 = \beta_1 = 0, \ \kappa_p = 0, \quad \text{and} \quad N_1 \in \{1, p\}.$$

Theorem 1 thus tells us that to determine the elliptic curves of conductor p, we are led to to find all binary cubic forms (reducible and irreducible) F of discriminant ± 4 and $\pm 4p$ and then solve the Thue equations

$$F(x,y) = 1 \quad \text{and} \quad F(x,y) = 8.$$

Since for any solution (x,y) to the equation $F(x,y) = 1$, we have $F(2x, 2y) = 8$, we may thus restrict our attention to the equation $F(x,y) = 8$ (where we assume that $\gcd(x,y) \mid 2$).

7.2. **Conductor $N = p^2$.** In case E has conductor $N = p^2$, we have that either E is a either a quadratic twist of a curve of conductor p, or we have $\nu_p(\Delta_E) \in \{2, 3, 4\}$. To see this, note that, via Table 3, $p \mid c_4$, $p \mid c_6$, and $\mathcal{D} \mid 2p$, and we may suppose that $(\nu_p(c_4(E)), \nu_p(c_6(E)), \nu_p(\Delta_E))$ is one of

$$(\geq 1, 1, 2), (1, \geq 2, 3), (\geq 2, 2, 4), (\geq 2, \geq 3, 6), (2, 3, \geq 7),$$
$$(\geq 3, 4, 8), (3, \geq 5, 9), (\geq 4, 5, 10).$$

In each case with $\nu_p(c_6(E)) \geq 3$, denote by E_1 the quadratic twist of E by $(-1)^{(p-1)/2}p$. For curves E with

$$(\nu_p(c_4(E)), \nu_p(c_6(E)), \nu_p(\Delta_E)) = (\geq 2, \geq 3, 6),$$

one may verify that E_1 has good reduction at p and hence conductor 1, a contradiction. If we have

$$(\nu_p(c_4(E)), \nu_p(c_6(E)), \nu_p(\Delta_E)) = (2, 3, \geq 7),$$

then

$$(\nu_p(c_4(E_1)), \nu_p(c_6(E_1)), \nu_p(\Delta_{E_1})) = (0, 0, \nu_p(\Delta_E) - 6)$$

and so E_1 has conductor p. In the remaining cases, where

$$(\nu_p(c_4(E)), \nu_p(c_6(E)), \nu_p(\Delta_E)) \in \{(\geq 3, 4, 8), (3, \geq 5, 9), (\geq 4, 5, 10)\},$$

we check that

$$(\nu_p(c_4(E_1)), \nu_p(c_6(E_1)), \nu_p(\Delta_{E_1})) \in \{(\geq 1, 1, 2), (1, \geq 2, 3), (\geq 2, 2, 4)\}.$$

It follows that, in order to determine all isomorphism classes of $E/\mathbb{Q}$ of conductor p^2, it suffices to carry out the following program:

- Find all curves of conductor p.
- Find $E/\mathbb{Q}$ with minimal discriminant $\Delta_E \in \{\pm p^2, \pm p^3, \pm p^4\}$, and then
- consider all appropriate quadratic twists of these curves.

The fact that we can essentially restrict attention to $E/\mathbb{Q}$ with minimal discriminant

$$\Delta_E \in \{\pm p^2, \pm p^3, \pm p^4\} \tag{34}$$

(once we have all curves of conductor p) was noted by Edixhoven, de Groot, and Top in Lemma 1 of [24]. To find the E satisfying (34), Theorem 1 (with specific appeal to (10)) leads us to consider Thue equations of the shape

$$F(x, y) = 8 \text{ for } F \text{ a form of discriminant } \pm 4p^2, \tag{35}$$

$$F(x, y) = 8p \text{ for } F \text{ a form of discriminant } \pm 4p, \tag{36}$$

and

$$F(x, y) = 8p \text{ for } F \text{ a form of discriminant } \pm 4p^2, \tag{37}$$

corresponding to $\Delta_E = \pm p^2$, $\pm p^3$ and $\pm p^4$, respectively.

TABLE 6. All curves of conductor p and p^2, for p prime, corresponding to reducible forms (i.e., with nontrivial rational 2-torsion). Note that t is any integer so that t^2+64 is prime. For the sake of brevity, we have omitted curves that are quadratic twists by $\pm p$ of curves of conductor p.

c_4	c_6	p	Δ_E	N_E
4353	287199	17	17	17
33	-81	17	17	17
t^2+48	$-t(t^2+72)$	t^2+64	t^2+64	t^2+64
273	4455	17	17^2	17
t^2-192	$-t(t^2+576)$	t^2+64	$-(t^2+64)^2$	t^2+64
1785	75411	7	7^3	7^2
105	1323	7	-7^3	7^2
33	12015	17	-17^4	17

7.3. **Reducible forms.** To find all elliptic curves $E/\mathbb{Q}$ with conductor p or p^2 arising from reducible forms, via Theorem 1 we are led to solve equations

$$F(x,y) = 8p^n \quad \text{with} \quad n \in \mathbb{Z} \quad \text{and} \quad \gcd(x,y) \mid 2, \tag{38}$$

where F is a reducible binary cubic form of discriminant ± 4, $\pm 4p$ and $\pm 4p^2$. This is an essentially elementary, though rather painful, exercise. Alternatively, we may observe that curves of conductor p or p^2 arising from reducible cubic forms are exactly those with at least one rational 2-torsion point. We can then use Theorem I of Hadano [29] to show that the only such p are $p = 7, 17$ and $p = t^2+64$ for integer t. In any case, after some rather tedious but straightforward work, we can show that the elliptic curves of conductor p or p^2 corresponding to reducible forms, are precisely those given in Table 6 (up to quadratic twists by $\pm p$).

7.4. **Irreducible forms: Conductor p.** A quick search demonstrates that there are no irreducible cubic forms of discriminant ± 4. Consequently, if we wish to find elliptic curves of conductor p coming from irreducible cubics in Theorem 1, we need to solve equations of the shape $F(x,y) = 8$ for all cubic forms of discriminant $\pm 4p$. An almost immediate consequence of this is the following.

Proposition 3. *Let $p > 17$ be prime. If there exists an elliptic curve $E/\mathbb{Q}$ of conductor p, then either $p = t^2+64$ for some integer t, or there exists an irreducible binary cubic form of discriminant $\pm 4p$.*

On the other hand, if we denote by $h(K)$ the class number of a number field K, classical results of Hasse [32] imply the following.

Proposition 4. *Let $p \equiv \pm 1 \pmod 8$ be prime and $\delta \in \{0,1\}$. If there exists an irreducible cubic form of discriminant $(-1)^\delta 4p$, then*

$$h\left(\mathbb{Q}(\sqrt{(-1)^\delta p})\right) \equiv 0 \pmod 3.$$

Combining Propositions 3 and 4, we thus have the following.

Corollary 5 (Theorem 1 of Setzer [57]). *Let $p \equiv \pm 1 \pmod 8$ be prime. If there exists an elliptic curve $E/\mathbb{Q}$ of conductor p, then either $p = t^2 + 64$ for some integer t, or we have*

$$h\left(\mathbb{Q}(\sqrt{p})\right) \cdot h\left(\mathbb{Q}(\sqrt{-p})\right) \equiv 0 \pmod 3.$$

We remark that Proposition 3 is actually a rather stronger criterion for guaranteeing the nonexistence of elliptic curves of conductor p than Corollary 5. Indeed, by way of example, we may readily check that there are no irreducible cubic forms of discriminant $\pm 4p$ for

$$p \in \{23, 31, 199, 239, 257, 367, 439\},$$

(and hence no elliptic curves of conductor p for these primes) while, in each case, we have that $3 \mid h\left(\mathbb{Q}(\sqrt{p})\right) \cdot h\left(\mathbb{Q}(\sqrt{-p})\right)$.

7.5. **Irreducible forms: Conductor p^2.** As noted earlier, to determine all elliptic curves of conductor p^2 for p prime, arising via Theorem 1 from irreducible cubics, it suffices to find those of conductor p and those of conductor p^2 with $\Delta_F = \pm p^2, \pm p^3$, and $\pm p^4$ (and subsequently twist them). We explore these cases below.

7.5.1. *Elliptic curves of discriminant $\pm p^3$.* To find elliptic curves of discriminant $\pm p^3$, we need to solve Thue equations of the shape $F(x, y) = 8p$, where F runs over all cubic forms of discriminant $\Delta_F = \pm 4p$. These forms are already required to compute curves of conductor p. Now, we can either proceed directly to solve $F(x, y) = 8p$ or transform the problem into one of solving a pair of new Thue equations of the shape $G_i(x, y) = 8$. In practice, we used the former when solving rigorously and the latter when solving heuristically (see Section 8.3).

We now describe this transformation. Let $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ be a reduced form of discriminant $\pm 4p$. Since $p \mid \Delta_F$, we have

$$F(x, y) \equiv a(x - r_0 y)^2(x - r_1 y) \pmod p,$$

where we must have that $p \nmid a$, since F is a reduced form (which implies that $1 \leq a < p$). Comparing coefficients of x shows that

$$2r_0 + r_1 \equiv -b/a \pmod p, \quad r_0^2 + 2r_0 r_1 \equiv c/a \pmod p$$

and

$$r_0^2 r_1 \equiv -d/a \pmod p.$$

Multiply the first two of these by a and add them to get

$$3ar_0^2 + 2br_0 + c \equiv 0 \pmod p.$$

We can solve this for r_0 and hence r_1:

$$(r_0, r_1) \equiv (3a)^{-1}(-b \pm t, -b \mp 2t) \pmod p,$$

where we require that t satisfies $t^2 \equiv b^2 - 3ac \pmod p$. Finding square roots modulo p can be done efficiently via the Tonelli-Shanks algorithm, for example (see, e.g., Shanks [59]), and almost trivially if, say, $p \equiv 3 \pmod 4$. Once we have these (r_0, r_1), we can readily check which pair satisfies $r_0^2 r_1 \equiv -d/a \pmod p$.

Now if $F(x, y) = 8p$, then we must have either

$$x \equiv r_0 y \pmod p \quad \text{or} \quad x \equiv r_1 y \pmod p.$$

In either case, write $x = r_i y + pu$, which maps the equation $F(x, y) = 8p$ to a pair of equations of the shape

$$G_i(u, y) = 8,$$

where

$$G_i(u, y) = ap^2u^3 + (3apr_i + bp)u^2y + (3ar_i^2 + 2br_i + c)uy^2 + \frac{1}{p}(ar_i^3 + br_i^2 + cr_i + d)y^3.$$

Notice that $\Delta_{G_i} = p^2\Delta_F$. In practice, for our deterministic approach, we will actually solve the equation $F(x, y) = 8p$ directly. For our heuristic approach (where a substantial increase in the size of the form's discriminant is not especially problematic), we will reduce to consideration of the equations $G_i(x, y) = 8$.

7.5.2. *A (conjecturally infinite) family of forms and solutions.* We note that there are families of primes for which we can guarantee that the equation $F(x, y) = 8p$ has solutions. By way of example, define a quartic form $p_{r,s}$ via

$$p_{r,s} = r^4 + 9r^2s^2 + 27s^4.$$

Then for a given r, s and $p = p_{r,s}$ the cubic form

$$F(x, y) = sx^3 + rx^2y - 3sxy^2 - ry^3$$

has discriminant $4p$. Additionally one can readily verify the polynomial identities

$$F(2r^2/s + 6s, -2r) = 8p \quad \text{and} \quad F(6s, -18s^2/r - 2r) = 8p.$$

If we set $s \in \{1, 2\}$ in the first of these, or $r \in \{1, 2\}$ in the second, then we arrive at four one-parameter families of forms of discriminant $4p$ for which the equation $F(x, y) = 8p$ has a solution, namely:

$$\begin{aligned}(p, x, y) = {} & (r^4 + 9r^2 + 27, 2r^2 + 6, -2r), (r^4 + 36r^2 + 432, r^2 + 12, -2r), \\ & (27s^4 + 9s^2 + 1, 6s, -18s^2 - 2), (27s^4 + 36s^2 + 16, 6s, -9s^2 - 4).\end{aligned}$$

Similarly, if we define

$$p_{r,s} = r^4 - 9r^2s^2 + 27s^4$$

then the form

$$F(x, y) = sx^3 + rx^2y + 3sxy^2 + ry^3$$

has discriminant $-4p$, and the equation $F(x, y) = 8p$ has solutions

$$(x, y) = (-2r^2/s + 6s, 2r) \text{ and } (6s, -18s^2/r + 2r)$$

and hence we again find (one-parameter) families of primes corresponding to either $r \in \{1, 2\}$ or $s \in \{1, 2\}$:

$$\begin{aligned}(p, x, y) = {} & (r^4 - 9r^2 + 27, -2r^2 + 6, 2r), (r^4 - 36r^2 + 432, -r^2 + 12, 2r), \\ & (27s^4 - 9s^2 + 1, 6s, -18s^2 + 2), (27s^4 - 36s^2 + 16, 6s, -9s^2 + 4).\end{aligned}$$

We expect that each of the quartic families described here attains infinitely many prime values, but proving this is beyond current technology.

7.5.3. *Elliptic curves of discriminant p^2 and p^4.* To find elliptic curves of discriminant p^2 and p^4 via Theorem 1, we need to solve Thue equations $F(x,y)=8$ and $F(x,y)=8p$, respectively, for cubic forms F of discriminant $4p^2$. Such forms are quite special and it turns out that they form a 2-parameter family.

Indeed, in order for there to exist a cubic form of discriminant $4p^2$, it is necessary and sufficient that we are able to write $p=r^2+27s^2$ for positive integers r and s, whereby F is equivalent to the form

$$F_{r,s}(x,y)=sx^3+rx^2y-9sxy^2-ry^3.$$

To see this, note that the existence of an irreducible cubic form of discriminant $4p^2$ for prime p necessarily implies that of a (cyclic) cubic field of discriminant p^2 and field index 2. From Silvester, Spearman, and Williams [60], there is a unique such field up to isomorphism, which exists precisely when the prime p can be represented by the quadratic form r^2+27s^2. We conclude as desired upon observing that

$$D_{F_{r,s}}=4\left(r^2+27s^2\right)^2.$$

It remains, then, to solve the Thue equations

$$F_{r,s}(x,y)=8 \quad \text{and} \quad F_{r,s}(x,y)=8p.$$

We can transform the problem of solving the second of these equations to one of solving a related Thue equation of the form $G_{r,s}(x,y)=8$. This transformation is quite similar to the one described in the previous subsection.

First note that we may assume that $p\nmid y$, since otherwise, we would require that $p\mid sx$, contradicting the facts that $s<\sqrt{p}$ and $p^2\nmid F$. Since $p^2\mid \Delta_F$, it follows that the congruence

$$su^3+ru^2-9su-r\equiv 0 \pmod{p}$$

has a unique solution modulo p; one may readily check that this satisfies $u\equiv 9s/r \pmod{p}$:

$$su^3+ru^2-9su-r\equiv -r^{-3}\cdot(r^2-27s^2)(r^2+27s^2)\equiv 0 \pmod{p}.$$

Consequently, we know that $x\equiv uy \pmod{p}$. Substituting $x=uy+vp$ into F gives

$$F_{r,s}(uy+vp,y)=a_0v^3+b_0v^2y+c_0vy^2+d_0y^3$$

so, with a quick renaming of variables, we obtain

$$G_{r,s}(x,y)=a_0x^3+b_0x^2y+c_0xy^2+d_0y^3=8,$$

where

$$a_0=sp^2,\quad b_0=(3us+r)p,\quad c_0=3u^2s+2ru-9s \quad \text{and} \quad d_0=(u^3s+ru^2-9us-r)/p.$$

A little algebra confirms that

$$\Delta_{G_{r,s}}=4p^4.$$

As noted in the previous subsection, we have solved $F_{r,s}(x,y)=8p$ directly in our deterministic approach, while we solved equation $G_{r,s}(x,y)=8$ for our heuristic method.

7.5.4. *Elliptic curves of discriminant $-p^2$ and $-p^4$.* Elliptic curves of discriminant $-p^2$ and $-p^4$ can be found through Theorem 1 by solving the Thue equations $F(x,y)=8$ and $F(x,y)=8p$, respectively, this time for cubic forms F of discriminant $-4p^2$. As in the cases treated in the preceding subsection, these forms can be described as a 2-parameter family. Specifically, such forms arise precisely when there exist integers r and s such that $p=|r^2-27s^2|$, in which case the form F is equivalent to

$$F_{r,s}(x,y)=sx^3+rx^2y+9sxy^2+ry^3.$$

The primes p for which we can write $p=|r^2-27s^2|$ are those with $p\equiv\pm1 \pmod{12}$. To see this, note first that if $p\equiv 1 \pmod 3$ and $p=|r^2-27s^2|$, then necessarily $p=r^2-27s^2$, so that $p\equiv 1 \pmod 4$, while, if $p\equiv -1 \pmod 3$ and $p=|r^2-27s^2|$, then $p=27s^2-r^2$ so that $p\equiv -1 \pmod 4$. It follows that necessarily $p\equiv\pm1 \pmod{12}$. To show that this is sufficient to have $p=|r^2-27s^2|$ for integers r and s, we appeal to the following.

Proposition 6. *If $p\equiv 1 \pmod{12}$ is prime, there exist positive integers r and s such that*

$$r^2-27s^2=p, \quad \text{with} \quad r<\frac{3}{2}\sqrt{6p} \quad \text{and} \quad s<\frac{5}{18}\sqrt{6p}.$$

If $p\equiv -1 \pmod{12}$ is prime, there exist positive integers r and s such that

$$r^2-27s^2=-p, \quad \text{with} \quad r<\frac{5}{2}\sqrt{2p} \quad \text{and} \quad s<\frac{1}{2}\sqrt{2p}.$$

This result is, in fact, an almost direct consequence of the following.

Theorem 7 (Theorem 112 from Nagell [47])**.** *If $p\equiv 1 \pmod{12}$ is prime, there exist positive integers u and v such that*

$$p=u^2-3v^2, \quad u<\sqrt{3p/2} \quad \text{and} \quad v<\sqrt{p/6}.$$

If $p\equiv -1 \pmod{12}$ is prime, there exist positive integers u and v such that

$$-p=u^2-3v^2, \quad u<\sqrt{p/2} \quad \text{and} \quad v<\sqrt{p/2}.$$

Proof of Proposition 6. If $p\equiv\pm1 \pmod{12}$, Theorem 7 guarantees the existence of integers u and v such that $p=|u^2-3v^2|$. If $3\mid v$, then we set $r=u, s=v/3$. Clearly, $3\nmid u$, so if $3\nmid v$, then we have (replacing v by $-v$ is necessary) that $u\equiv v \pmod 3$. If we now set $r=2u+3v$ and $s=(2v+u)/3$, then it follows that

$$|r^2-27v^2|=|(2u+3v)^2-3(2v+u)^2|=|u^2-3v^2|=p$$

and hence either

$$|r|\le 2\sqrt{3p/2}+3\sqrt{p/6}=\frac{3}{2}\sqrt{6p} \quad \text{and} \quad |s|\le\frac{1}{3}(2\sqrt{p/6}+\sqrt{3p/2})=\frac{5}{18}\sqrt{6p},$$

or

$$|r|\le 2\sqrt{p/2}+3\sqrt{p/2}=\frac{5}{2}\sqrt{2p} \quad \text{and} \quad |s|\le\frac{1}{3}(2\sqrt{p/2}+\sqrt{p/2})=\frac{1}{2}\sqrt{2p}. \quad \square$$

Again, we are able to reduce the problem of solving $F_{r,s}(x,y)=8p$ to that of treating a related equation $G_{r,s}(x,y)=8$. As before, note that if $u\equiv -9s/r \pmod p$, then

$$su^3+ru^2+9su+r\equiv r^{-3}(r^2-27s^2)(r^2+27s^2)\equiv 0 \pmod p.$$

Again, write $x = r_0 y + vp$ so that, after renaming v, we have

$$G_{r,s}(x,y) = a_0 x^3 + b_0 x^2 y + c_0 x y^2 + d_0 y^3 = 8,$$

where

$$a_0 = sp^2, \quad b_0 = (3us+r)p, \quad c_0 = 3u^2 s + 2ru + 9s, \quad \text{and} \quad d_0 = (u^3 s + ru^2 + 9us + r)/p.$$

Note that, in contrast to the case where $p = r^2 + 27s^2$, here p is represented by an indefinite quadratic form and so the presence of infinitely many units in $\mathbb{Q}(\sqrt{3})$ implies that a given representation is not unique. If, however, we have two solutions to the equation $|r^2 - 27s^2| = p$, say (r_1, s_1) and (r_2, s_2), then the corresponding forms

$$s_1 x^3 + r_1 x^2 y + 9 s_1 x y^2 + r_1 y^3 \quad \text{and} \quad s_2 x^3 + r_2 x^2 y + 9 s_2 x y^2 + r_2 y^3$$

may be shown to be $\mathrm{GL}_2(\mathbb{Z})$-equivalent.

8. Computational details

As noted earlier, the computations required to generate curves of prime conductor p (and subsequently conductor p^2) fall into a small number of distinct parts.

8.1. **Generating the required forms.** To find the irreducible forms potentially corresponding to elliptic curves of prime conductor $p \leq X$ for some fixed positive real X, arguing as in Section 5, we tabulated all reduced forms $F(x,y) = ax^3 + bx^2 y + cxy^2 + d$ with discriminants in $(0, 4X]$ and $[-4X, 0)$, separately. As each form was generated, we checked to see if it actually satisfied the desired definition of reduction. Of course, this does not only produce forms with discriminant $\pm 4p$; as each form was produced, we kept only those whose discriminant was in the appropriate range, and equal to $\pm 4p$ for some prime p. Checking primality was done using the Miller-Rabin primality test (see [44], [54]; to make this deterministic for the range we require, we appeal to [61]). While it is straightforward to code the above in computer algebra packages such as `sage` [56], `maple` [7] or Magma [9], we instead implemented it in `c++` for speed. To avoid possible numerical overflows, we used the `CLN` library [30] for `c++`.

We computed forms of discriminant $\pm 4p$ in two separate runs—first to $p \leq 10^{12}$ and then a second run to $p \leq 2 \times 10^{13}$. In the first of these, we constructed all the forms and explicitly saved them to files. Constructing all the required positive discriminant forms took approximately 40 days of CPU time on a modern server, and about 300 gigabytes of disc space. Thankfully, the computation is easily parallelized and it only took about 1 day of real time. We split the jobs by running a manager which distributed a-values to the other cores. The output from each a-value was stored as a tab-delimited text file with one tuple of p, a, b, c, d on each line. Generating all forms of negative discriminant took about 3 times longer and required about 900 gigabytes of disc space. The distribution of forms is heavily weighted to small values of a. To allow us to spread the load across many CPUs we actually split the task into 2 parts. We first ran $a \geq 3$, with the master node distributing a-values to the other cores. We then ran $a = 1$ and 2 with the master node distributing b-values to the other cores. The total CPU time was about three times longer than for the positive case (there being essentially three times as many forms), but more real time was required due to these complications. Thus generating all forms took less than 1 week of real time but required about 1.2 terabytes of disc space.

These forms were then sorted by discriminant while keeping positive and negative discriminant forms separated. Sorting a terabyte of data is a nontrivial task, and in practice we did this by first sorting[1] the forms for each a-value and then splitting them into files of discriminants in the ranges $[n \times 10^9, (n+1) \times 10^9)$ for $n \in [0, 999]$. Finally, all the files of each discriminant range were sorted together. This process for positive and negative discriminant forms took around two days of real time. We found 9247369050 forms of positive discriminant $4p$ and 27938060315 of negative discriminant $-4p$, with p bounded by 10^{12}. Of these, 475831852 and 828238359, respectively, had $F(x, y) = 8$ solvable (by the heuristic method described below), leading to 159552514 and 276339267 elliptic curves of positive and negative discriminant, respectively, with prime conductor up to 10^{12}.

The second run to $p \leq 2 \times 10^{13}$ required a different workflow due to space constraints. Saving all forms to disc was simply impractical—we estimated it to require over 20 terabytes of space! Because of this we combined the form-generation code with the heuristic solution method (see below) and kept only those forms $F(x, y)$ for which solutions to $F(x, y) = 8$ existed. Since only a small fraction of forms (asymptotically likely 0) have solutions, the disc space required was considerably less. Indeed to store all the required forms took about 250 and 400 gigabytes for positive and negative forms, respectively. This then translated into about 65 and 115 gigabytes of positive and negative discriminant curves, respectively, with prime conductor up to 2×10^{13}. This second computation took roughly 20 times longer than the first, requiring about 4 months of real time. This led to a final count of 1738595275 and 3011354026 (isomorphism classes of) curves of positive and negative discriminant, respectively, with prime conductor up to 2×10^{13}.

8.2. **Complete solution of Thue equations: Conductor p.** For each form encountered, we needed to solve the Thue equation

$$ax^3 + bx^2y + cxy^2 + dy^3 = 8$$

in integers x and y with $\gcd(x, y) \in \{1, 2\}$. We approached this in two distinct ways.

To solve the Thue equation rigorously, we appealed to by now well-known arguments of Tzanakis and de Weger [67], based upon lower bounds for linear forms in complex logarithms, together with lattice basis reduction; these are implemented in several computer algebra packages, including Magma [9] and Pari/GP [50]. The main computational bottleneck in this approach is typically that of computing the fundamental units in the corresponding cubic fields; for computations p of size up to 10^9 or so, we encountered no difficulties with any of the Thue equations arising (in particular, the fundamental units occurring can be certified without reliance upon the Generalized Riemann Hypothesis).

We ran this computation in Magma [9], using its built-in Thue equation solver. Due to memory consumption issues, we fed the forms into Magma in small batches, restarting Magma after each set. We saved the output as a tuple

$$p, a, b, c, d, n, \{(x_1, y_1), \ldots, (x_n, y_n)\},$$

where p, a, b, c, d came from the form, n counts the number of solutions of the Thue equation and (x_i, y_i) the solutions. These solutions can then be converted

[1] Using the standard unix `sort` command and taking advantage of multiple cores.

into corresponding elliptic curves in minimal form using Theorem 1 and standard techniques.

For positive discriminant, this approach works without issue for $p < 10^{10}$. For forms of negative discriminant $-4p$, however, the fundamental unit ϵ_p in the associated cubic field can be extremely large (i.e., $\log|\epsilon_p|$ can be roughly of size $\sqrt{p}$). For this reason, finding all negative discriminant curves with prime conductor exceeding $2 \cdot 10^9$ or so proves to be extremely time-consuming. Consequently, for large p, we turned to a nonexhaustive method, which, though it finds solutions to the Thue equation, is not actually guaranteed to find them all.

8.3. **Nonexhaustive, heuristic solution of Thue equations.** If we wish to find all "small" solutions to a Thue equation (which, subject to various well-accepted conjectures, might actually prove to be all solutions), there is an obvious and very computationally efficient approach we can take, based upon the idea that, given any solution to the equation $F(x, y) = m$ for fixed integer m, we necessarily either have that x and y are (very) small, relative to m, or that x/y is a convergent in the infinite simple continued fraction expansion to a root of the equation $F(x, 1) = 0$.

Such techniques were developed in detail by Pethő [52], [53]; in particular, he provides a precise and computationally efficient distinction between "large" and "small" solutions. Following this, for each form F under consideration, we expanded the roots of $F(x, 1) = 0$ to high precision, again using the `CLN` library for `c++`. We then computed the continued fraction expansion for each real root, along with its associated convergents. Each convergent x/y was then substituted into $F(x, y)$ and checked to see if $F(x, y) = \pm 1, \pm 8$. Replacing (x, y) by one of $(-x, -y), (2x, 2y)$ or $(-2x, -2y)$, if necessary, then provided the required solutions of $F(x, y) = 8$. The precision was chosen so that we could compute convergents x/y with $|x|, |y| \leq 2^{128} \approx 3.4 \times 10^{38}$. We then looked for solutions of small height using a brute force search over a relatively small range of values.

To "solve" $F(x, y) = 8$ by this method, for all forms with discriminant $\pm 4p$ with $p \leq 10^{12}$, took about 1 week of real time using 80 cores. The resulting solutions files (in which we stored also forms with no corresponding solutions) required about 1.5 terabytes of disc space. Again, the files were split into files of absolute discriminant (or more precisely absolute discriminant divided by 4) in the ranges $[n \times 10^9, (n + 1) \times 10^9)$ for $n \in [0, 999]$. For the second computation run to $p \leq 2 \times 10^{13}$, we combined the form-generation and heuristic-solutions steps, storing only forms which had solutions. This produced about 235 and 405 gigabytes of data for positive and negative discriminants, respectively.

8.4. **Conversion to curves.** Once one has a tuple (a, b, c, d, x, y), one then computes $G_F(x, y)$ and $H_F(x, y)$, appeals to Theorem 1 and checks twists. This leaves us with a list of pairs (c_4, c_6) corresponding to elliptic curves. It is now straightforward to derive a_1, a_2, a_3, a_4 and a_6 for a corresponding elliptic curve in minimal form (see, e.g., Cremona [16]). For each curve, we saved a tuple $p, a_1, a_2, a_3, a_4, a_6, \pm 1$ with the last entry being the sign of the discriminant of the form used to generate the curve (which coincides with the sign of the discriminant of the curve). We then merged the curves with positive and negative discriminants and added the curves with prime conductor arising from reducible forms (i.e., of small conductor or for primes of the form $t^2 + 64$). After sorting by conductor, this formed a single file

of about 17 gigabytes for all curves with prime conductor $p < 10^{12}$ and about 180 gigabytes for all curves with conductor $p < 2 \times 10^{13}$.

8.5. **Conductor p^2.** The conductor p^2 computation was quite similar, but was split further into parts.

8.5.1. *Twisting conductor p.* The vast majority of curves of conductor p^2 that we encountered arose as quadratic twists of curves of conductor p. To compute these, we took all curves with conductor $p \leq 10^{10}$ and calculated the invariants c_4 and c_6. The twisted curve then has corresponding c-invariants

$$c_4' = p^2 c_4 \quad \text{and} \quad c_6' = (-1)^{(p-1)/2} p^3 c_6.$$

The minimal a-invariants were then computed as for curves of conductor p.

We wrote a simple `c++` program to read curves of conductor p and then twist them, recompute the a-invariants and output them as a tuple $p^2, a_1, a_2, a_3, a_4, a_6, \pm 1$. The resulting code only took a few minutes to process the approximately 1.1×10^7 curves.

8.5.2. *Solving $F(x, y) = 8p$ with F of discriminant $\pm 4p$.* There was no need to retabulate forms for this computation; we reused the positive and negative forms of discriminant $\pm 4p$ with $p \leq 10^{10}$ from the conductor-p computations. We subsequently rigorously solved the corresponding equations $F(x, y) = 8p$ for $p \leq 10^8$. To solve the Thue equation $F(x, y) = 8p$ for $10^8 < p \leq 10^{10}$, using the nonexhaustive, heuristic method, we first converted the equation to a pair of new Thue equations of the form $G_i(u, y) = 8$ as described in Section 7.5.1 and then applied Pethő's solution search method (where we searched for solutions to these new equations with $|y|$ bounded by 2^{128} and $|u| = |(x - r_i y)/p|$ bounded in such way as to guarantee that our original $|x|$ is also bounded by 2^{128}).

The solutions were then processed into curves as for the conductor p case above, and the resulting curves were twisted by $\pm p$ in order to obtain more curves of conductor p^2.

8.5.3. *Solving $F(x, y) \in \{8, 8p\}$ with F of discriminant $\pm 4p^2$.* To find forms of discriminant $4p^2$ with $p \leq 10^{10}$ we need only check to see which primes are of the form $p = r^2 + 27s^2$ in the desired range. To do so, we simply looped over r and s values and then again checked primality using Miller-Rabin. As each prime was found, the corresponding p, r, s tuple was converted to a form as in Section 7.5.3, and the Thue equations $F(x, y) = 8$ and $F(x, y) = 8p$ were solved, using the rigorous approach for $p < 10^6$ and the nonexhaustive method described previously for $10^6 < p \leq 10^{10}$. Again, in the latter situation, the equation $F(x, y) = 8p$ was converted to a new equation $G(x, y) = 8$ as described in Section 7.5.3. The process for forms of discriminant $-4p^2$ was very similar, excepting that more care is required with the range of r and s (appealing to Proposition 6). The nonexhaustive method solving both $F(x, y) = 8$ and $F(x, y) = 8p$ for positive and negative forms took a total of approximately 5 days of real time on a smaller server of 20 cores. The rigorous approach, even restricted to prime $p < 10^6$ was much, much slower.

The solutions were then converted to curves as with the previous cases and each resulting curve was twisted by $\pm p$ to find other curves of conductor p^2.

9. Data

9.1. **Previous work.** The principal prior work on computing the table of elliptic curves of a prime conductor was carried out in two lengthy computations, by Brumer and McGuinness [11] in the late 1980s and by Stein and Watkins [63] slightly more than ten years later. For the first of these computations, the authors fixed the a_1, a_2, and a_3 invariants (12 possibilities) and looped over a_4 and a_6 chosen to make the corresponding discriminant small. By this approach, they were able to find 311243 curves of prime conductor $p < 10^8$ (representing approximately 99.6% of such curves). In the latter case, the authors looped instead over c_4 and c_6, subject to (necessary) local conditions. They obtained a large collection of elliptic curves of general conductor to 10^8, and 11378912 of those with prime conductor to 10^{10} (which we estimate to be slightly in excess of 99.8% of such curves).

9.2. **Counts: Conductor p.** By way of comparison, we found the following numbers of isomorphism classes of elliptic curves over $\mathbb{Q}$ with prime conductor $p \le X$:

X	$\Delta_E > 0$	$\Delta_E < 0$	Ratio^2	Total	Expected	Total / Expected
10^3	33	51	2.3884	84	68	1.2353
10^4	129	228	3.1239	357	321	1.1122
10^5	624	1116	3.1986	1740	1669	1.0425
10^6	3388	5912	3.0450	9300	9223	1.0084
10^7	19605	34006	3.0087	53611	52916	1.0131
10^8	114452	198041	2.9941	312493	311587	1.0029
10^9	685278	1187686	3.0038	1872964	1869757	1.0017
2×10^9	1178204	2040736	3.0001	3218940	3216245	1.0008
10^{10}	4171055	7226982	3.0021	11398037	11383665	1.0013
10^{11}	25661634	44466339	3.0026	70127973	70107401	1.0003
10^{12}	159552514	276341397	2.9997	435893911	435810488	1.0002
10^{13}	999385394	1731017588	3.0001	2730402982	2730189484	1.00008
2×10^{13}	1738595275	3011354026	3.0000	4749949301	4749609116	1.00007

The data above the line is rigorous; for positive discriminant, we actually have a rigorous result to 10^{10}. For the positive forms this took about one week of real time using 80 cores. Unfortunately, the negative discriminant forms took significantly longer, roughly 2 months of real time using 80 cores. Heuristics given by Brumer and McGuinness [11] suggest that the number of elliptic curves of negative discriminant of absolute discriminant up to X should be asymptotically $\sqrt{3}$ times as many as those of positive discriminant in the same range; here we report the square of this ratio in the given ranges. The aforementioned heuristic count of Brumer and McGuinness suggests that the expected number of E with prime $N_E \le X$ should be

$$\frac{\sqrt{3}}{12}\left(\int_1^\infty \frac{1}{\sqrt{u^3-1}}du + \int_{-1}^\infty \frac{1}{\sqrt{u^3+1}}du\right)\ \mathrm{Li}(X^{5/6}),$$

which we list (after rounding) in the table above. It should not be surprising that this "expected" number of curves appears to slightly undercount the actual number, since it does not take into account the roughly $\sqrt{X}/\log X$ curves of conductor $p = n^2 + 64$ and discriminant $-p^2$ (counting only curves of discriminant $\pm p$).

9.3. **Counts: conductor p^2.** To compile the final list of curves of conductor p^2, we combined the five lists of curves: twists of curves of conductor p, curves from forms of discriminant $+4p$ and $-4p$, and curves from discriminant $+4p^2$ and $-4p^2$. The

list was then sorted and any duplicates removed. The resulting list is approximately one gigabyte in size. The counts of curves are as follows; here we list numbers of isomorphism classes of curves of conductor p^2 for p prime with $p \leq X$:

X	$\Delta_E > 0$	$\Delta_E < 0$	Total	Ratio^2
10^3	53	93	146	3.0790
10^4	191	322	513	2.8421
10^5	764	1304	2068	2.9132
10^6	3764	6356	10120	2.8515
10^7	20539	35096	55635	2.9198
10^8	116894	200799	317693	2.9508
10^9	691806	1195262	1887068	2.9851
10^{10}	4189445	7247980	11437425	2.9931

Subsequently we decided that we should recompute the discriminants of these curves as a sanity check, by reading the curves into `sage` and using its built-in elliptic curve routines to compute and then factor the discriminant. This took about one day on a single core.

The only curves of genuine interest are those that do not arise from twisting, i.e., those of discriminant $\pm p^2$, $\pm p^3$ and $\pm p^4$. In the last of these categories, we found only 5 curves, of conductors 11^2, 43^2, 431^2, 433^2. and 33013^2. The first four of these were noted by Edixhoven, de Groot, and Top [24] (and are of small enough conductor to now appear in Cremona's tables). The fifth, satisfying

$$(a_1, a_2, a_3, a_4, a_6) = (1, -1, 1, -1294206576, 17920963598714),$$

has discriminant 33013^4. For discriminants $\pm p^2$ and $\pm p^3$, we found the following numbers of curves, for conductors p^2 with $p \leq X$:

X	$\Delta_E = -p^2$	$\Delta_E = p^2$	$\Delta_E = -p^3$	$\Delta_E = p^3$
10^3	12	4	7	4
10^4	36	24	9	5
10^5	80	58	12	9
10^6	203	170	17	15
10^7	519	441	24	23
10^8	1345	1182	32	36
10^9	3738	3203	48	58
10^{10}	10437	9106	60	86

It is perhaps worth observing that the majority of these curves arise from, in the case of discriminant $\pm p^2$, forms with, in the notation of Sections 7.5.3 and 7.5.4, either r or s in $\{1, 8\}$. Similarly, for $\Delta_E = \pm p^3$, most of the curves we found come from forms in the eight one-parameter families described in Section 7.5.1. We are unaware of a heuristic predicting the number of curves of conductor p^2 up to X that do not arise from twisting curves of conductor p.

9.4. **Thue equations.** It is noteworthy that all solutions we encountered to the Thue equations $F(x, y) = 8$ and $F(x, y) = 8p$ under consideration satisfied $|x|, |y| < 2^{30}$. The "largest" such solution corresponded to the equation

$$355x^3 + 293x^2y - 1310xy^2 - 292y^3 = 8,$$

where we have

$$(x, y) = (188455233, -82526573).$$

This leads to the elliptic curve of conductor 948762329069,

$$E \;:\; y^2 + xy + y = x^2 - 2x^2 + a_4 x + a_6,$$

with

$$a_4 = -1197791024934480813341$$

and

$$a_6 = 1595584083717556524357956436864 1.$$

Note that this curve does not actually correspond to a particularly impressive *abc* or Hall conjecture (see Section 10 for the definition of this term) example.

In the following table, we collect data on the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible binary cubic forms of discriminant $4p$ or $-4p$ for p in $[0, X]$, denoted $P_3(0, X)$ and $P_3(-X, 0)$, respectively. We also provide counts for those forms where the corresponding equation $F(x, y) = 8$ has at least one integer solution, denoted $P_3^*(0, X)$ and $P_3^*(-X, 0)$ for positive and negative discriminant forms, respectively:

X	$P_3(0,X)$	$P_3^*(0,X)$	$P_3(-X,0)$	$P_3^*(-X,0)$
10^3	23	22	78	61
10^4	204	163	740	453
10^5	1851	1159	6104	2641
10^6	16333	7668	53202	16079
10^7	147653	49866	466601	97074
10^8	1330934	314722	4126541	582792
10^9	12050910	1966105	36979557	3530820
2×10^9	23418535	3408656	71676647	6080245
10^{10}	109730653	12229663	334260481	21576585
10^{11}	1004607003	76122366	3045402451	133115651
10^{12}	9247369050	475831852	27938060315	828238359

Due to space limitations we did not compute these statistics in the second large computational run.

Our expectation is that the number of forms for which the equation $F(x, y) = 8$ has solutions with absolute discriminant up to X is $o(X)$ (i.e., this occurs for essentially "zero" percent of forms; a first step in proving something is this direction can be found in recent work of Akhtari and Bhargava [2]).

9.5. **Elliptic curves with the same prime conductor.** One might ask how many isomorphism classes of curves of a given prime conductor can occur. If one accepts recent heuristics that predict that the Mordell-Weil rank of $E/\mathbb{Q}$ is absolutely bounded (see, e.g., [51] and [70]), then this number should also be so bounded. As noted by Brumer and Silverman [12], there are 13 curves of conductor 61263451. Up to $p < 10^{12}$, the largest number we encountered was for $p = 530956036043$, with

20 isogeny classes, corresponding to $(a_1, a_2, a_3, a_4, a_6)$ as follows:

$(0, -1, 1, -1003, 37465)$, $(0, -1, 1, -1775, 45957)$, $(0, -1, 1, -38939, 2970729)$,
$(0, -1, 1, -659, -35439)$, $(0, -1, 1, 2011, 4311)$, $(0, -2, 1, -27597, -1746656)$,
$(0, -2, 1, 57, 35020)$, $(1, -1, 0, -13337473, 18751485796)$, $(0, 0, 1, -13921, 633170)$,
$(0, 0, 1, -30292, -2029574)$, $(0, 0, 1, -6721, -214958)$,
$(0, 0, 1, -845710, -299350726)$, $(0, 0, 1, -86411851, 309177638530)$,
$(0, 0, 1, -10717, 428466)$, $(1, -1, 0, -5632177, 5146137924)$, $(1, -1, 0, 878, 33379)$,
$(1, -1, 1, 1080, 32014)$, $(1, -2, 1, -8117, -278943)$,
$(1, -3, 0, -2879, 71732)$, $(1, -3, 0, -30415, -2014316)$.

All have discriminant $-p$. Elkies [25] found examples of rather larger conductor with more curves, including 21 classes for $p = 14425386253757$ and discriminant p, and 24 classes for $p = 998820191314747$ and discriminant $-p$. Our computations confirm, with high likelihood, that, for $p < 2 \times 10^{13}$, the number of isomorphism classes of elliptic curves of conductor a fixed prime p is at most 21.

9.6. **Rank and discriminant records.** In the following table, we list the smallest prime conductor with a given Mordell-Weil rank. These were computed by running through our data, using Rubinstein's upper bounds for analytic ranks (as implemented in Sage) to search for candidate curves of "large" rank which were then checked using mwrank [18]. The last entry corresponds to a curve of rank 6 with minimal positive prime discriminant; we have not yet ruled out the existence of a rank 6 curve with smaller absolute (negative) discriminant.

N	$(a_1, a_2, a_3, a_4, a_6)$	$\text{sign}(\Delta_E)$	$rk(E(\mathbb{Q}))$
37	$(0, 0, 1, -1, 0)$	$+$	1
389	$(0, 1, 1, -2, 0)$	$+$	2
5077	$(0, 0, 1, -7, 6)$	$+$	3
501029	$(0, 1, 1, -72, 210)$	$+$	4
19047851	$(0, 0, 1, -79, 342)$	$-$	5
6756532597	$(0, 0, 1, -547, -2934)$	$+$	6

It is perhaps noteworthy that the curve listed here of rank 6 has the smallest known minimal discriminant for such a curve (see Table 4 of Elkies and Watkins [27]).

If we are interested in similar records over all curves, including composite conductors, we have

N	$(a_1, a_2, a_3, a_4, a_6)$	$\text{sign}(\Delta_E)$	$rk(E(\mathbb{Q}))$
37	$(0, 0, 1, -1, 0)$	$+$	1
389	$(0, 1, 1, -2, 0]$	$+$	2
5077	$(0, 0, 1, -7, 6)$	$+$	3
234446	$(1, -1, 0, -79, 289)$	$+$	4
19047851	$(0, 0, 1, -79, 342)$	$-$	5
5187563742	$(1, 1, 0, -2582, 48720)$	$+$	6
382623908456	$(0, 0, 0, -10012, 346900)$	$+$	7

Here, the curves listed above the line are proven to be those of smallest conductor with the given rank. Those listed below the line have the smallest known conductor for the corresponding rank. It is our belief that the techniques of this paper should enable one to determine whether the curve listed here of rank 5 has the smallest conductor of any curve with this property.

10. Completeness of our data

As a final result, we will present something that might, optimistically, be viewed as evidence that our "heuristic" approach, in practice, enables us to actually find all elliptic curves of prime conductor $p < 2 \times 10^{13}$.

A conjecture of Hall, admittedly one that without modification is widely disbelieved at present, is that if x and y are integers for which $x^3 - y^2$ is nonzero, then the *Hall ratio*

$$\mathcal{H}_{x,y} = \frac{|x|^{1/2}}{|x^3 - y^2|}$$

is absolutely bounded. The pair (x, y) corresponding to the largest known Hall ratio comes from the identity

$$5853886516781223^3 - 447884928428402042307918^2 = 1641843,$$

noted by Elkies [26], with $\mathcal{H}_{x,y} > 46.6$. All other examples known currently have $\mathcal{H}_{x,y} < 7$. We prove the following.

Proposition 8. *If there is an elliptic curve E with conductor $p < 2 \times 10^{13}$, corresponding via Theorem 1 to a cubic form F and $u, v \in \mathbb{Z}$, such that*

$$F(u, v) = 8 \quad \textit{and} \quad \max\{|u|, |v|\} \geq 2^{128},$$

then

$$\mathcal{H}_{c_4(E),c_6(E)} > 1.5 \times 10^6. \tag{39}$$

In other words, if there is an elliptic curve E with conductor $p < 2 \times 10^{13}$ that we have missed in our heuristic search, then we necessarily have inequality (39) (and hence a record-setting Hall ratio).

Proof. The main idea behind our proof is that the roots of the Hessian $H_F(x, 1)$ have no particularly good reason to be close to those of the polynomial $F(x, 1)$. It follows that, if we have relatively large integers u and v satisfying the Thue equation $F(u, v) = 8$ (so that u/v is close to a root of $F(x, 1) = 0$), our expectation is that not only does $H_F(u, v)$ fail to be small, but, in fact, we should have inequalities of the order of

$$H_F(u, v) \gg (\max\{|u|, |v|\})^2 \quad \text{and} \quad G_F(u, v) \gg (\max\{|u|, |v|\})^3$$

(where the Vinogradov symbol hides a possible dependence on p). Since

$$c_4(E) = \mathcal{D}^2 H_F(u, v) \text{ and } c_6(E) = -\frac{1}{2}\mathcal{D}^3 G_F(u, v),$$

where $\mathcal{D} \in \{1, 2\}$, these would imply that

$$\mathcal{H}_{c_4(E),c_6(E)} \gg_p \frac{1}{p} \max\{|u|, |v|\}.$$

In fact, for forms (and curves) of positive discriminant, we can deduce inequalities of the shape

$$\mathcal{H}_{c_4(E),c_6(E)} \gg_p p^{-3/4} \min\{|u|, |v|\} \gg p^{-5/4} \max\{|u|, |v|\},$$

where the implicit constants are absolute. For curves of negative discriminant, we have a slightly weaker result:

$$\mathcal{H}_{c_4(E),c_6(E)} \gg_p p^{-1} \min\{|u|, |v|\} \gg p^{-3/2} \max\{|u|, |v|\}.$$

To make this argument precise, let us write, for concision, $c_4 = c_4(E)$ and $c_6 = c_6(E)$. From the identity $|c_4^3 - c_6^2| = 1728p$, we have a Hall ratio

$$\mathcal{H}_{c_4,c_6} = \frac{|c_4|^{1/2}}{1728p} > \frac{|c_4|^{1/2}}{3.456 \times 10^{16}} \geq \frac{|H_F(u,v)|^{1/2}}{3.456 \times 10^{16}}.$$

Our goal will thus be to obtain a lower bound upon $|H_F(u,v)|$; we claim that, in fact, $|H_F(u,v)| > 3 \times 10^{45}$, whereby this Hall ratio exceeds 1.5×10^6, as stated. Suppose that we have a cubic form F and integers u and v with $D_F = \pm 4p$ for p prime,

$$\max\{|u|,|v|\} \geq 2^{128} \quad \text{and} \quad 2 \times 10^9 < p < 2 \times 10^{13}. \tag{40}$$

Notice that $F(u,0) = \omega_0 u^3 = 8$ and hence (40) implies that $v \neq 0$.

Write

$$F(u,v) = \omega_0(u - \alpha_1 v)(u - \alpha_2 v)(u - \alpha_3 v)$$

and suppose that

$$|u - \alpha_1 v| = \min\{|u - \alpha_i v|,\ i = 1,2,3\}.$$

We may further assume, without loss of generality, that the form F is reduced. From (6), we have

$$\omega_0^2\ |H_F(\alpha_1,1)\, H_F(\alpha_2,1)\, H_F(\alpha_3,1)| = 16\, p^2. \tag{41}$$

For future use, we note that the main result of Mahler [40] implies the inequality

$$|\omega_0| \prod_{i=1}^{3} \max\{1,|\alpha_i|\} \leq |\omega_0| + |\omega_1| + |\omega_2| + |\omega_3|. \tag{42}$$

Let us assume first that $D_F > 0$, whereby H_F has negative discriminant ($D_{H_F} = -3D_F$). Since F is reduced, we have

$$|\omega_1\omega_2 - 9\omega_0\omega_3| \leq \omega_1^2 - 3\omega_0\omega_2 \leq \omega_2^2 - 3\omega_1\omega_3,$$

and hence the identity

$$(\omega_1\omega_2 - 9\omega_0\omega_3)^2 - 4(\omega_1^2 - 3\omega_0\omega_2)(\omega_2^2 - 3\omega_1\omega_3) = -3D_F \tag{43}$$

yields the inequalities

$$D_F \geq (\omega_1^2 - 3\omega_0\omega_2)(\omega_2^2 - 3\omega_1\omega_3) \geq (\omega_1^2 - 3\omega_0\omega_2)^2. \tag{44}$$

Since (43) and $D_F > 0$ imply that $\omega_1^2 - 3\omega_0\omega_2 \neq 0$, we may write

$$\frac{H_F(\alpha_1,1)}{\omega_1^2 - 3\omega_0\omega_2} = \left(\alpha_1 - \frac{9\omega_0\omega_3 - \omega_1\omega_2 + \sqrt{-3D_F}}{2(\omega_1^2 - 3\omega_0\omega_2)}\right)\left(\alpha_1 - \frac{9\omega_0\omega_3 - \omega_1\omega_2 - \sqrt{-3D_F}}{2(\omega_1^2 - 3\omega_0\omega_2)}\right).$$

Defining

$$\Gamma_1 = \alpha_1 - \frac{9\omega_0\omega_3 - \omega_1\omega_2}{2(\omega_1^2 - 3\omega_0\omega_2)} \quad \text{and} \quad \Gamma_2 = \frac{\sqrt{3D_F}}{2(\omega_1^2 - 3\omega_0\omega_2)},$$

we have

$$H_F(\alpha_1,1) = \left(\omega_1^2 - 3\omega_0\omega_2\right)\left(\Gamma_1^2 + \Gamma_2^2\right)$$

and so

$$|H_F(\alpha_1,1)| > \frac{3D_F}{4(\omega_1^2 - 3\omega_0\omega_2)}. \tag{45}$$

Since α_1 is "close" to u/v, it follows that the same is true for $H_F(\alpha_1, 1)$ and $H_F(u/v, 1) = v^{-2}H_F(u, v)$. To make this precise, note that, via the Mean Value Theorem,

$$|H_F(\alpha_1, 1) - H_F(u/v, 1)| = \left|2(\omega_1^2 - 3\omega_0\omega_2)y + \omega_1\omega_2 - 9\omega_0\omega_3\right| \left|\alpha_1 - \frac{u}{v}\right|, \tag{46}$$

for some y lying between α_1 and u/v. We thus have

$$|H_F(\alpha_1, 1) - H_F(u/v, 1)| \leq (\omega_1^2 - 3\omega_0\omega_2)\left(2\left(|\alpha_1| + \left|\alpha_1 - \frac{u}{v}\right|\right) + 1\right)\left|\alpha_1 - \frac{u}{v}\right|. \tag{47}$$

To derive an upper bound upon $\left|\alpha_1 - \frac{u}{v}\right|$, we can argue as in the proof of Theorem 2 of Pethő [53] to obtain the inequality

$$\left|\alpha_1 - \frac{u}{v}\right| \leq 2^{7/3}D_F^{-1/6}v^{-2}. \tag{48}$$

Since $|v| \geq 1$ and $D_F = 4p > 8 \times 10^9$, we thus have that

$$\left|\alpha_1 - \frac{u}{v}\right| < 0.12. \tag{49}$$

We may suppose that F is reduced, whereby, crudely, from Lemma 3.5 of Belebas [3],

$$|\omega_0| \leq \frac{2D_F^{1/4}}{3\sqrt{3}} \quad \text{and} \quad |\omega_1| \leq \frac{3\omega_0}{2} + \left(\sqrt{D_F} - \frac{27\omega_0^2}{4}\right)^{1/2} < \left(1 + \frac{1}{\sqrt{3}}\right)D_F^{1/4}.$$

From Proposition 5.5 of Belabas and Cohen [4],

$$|\omega_2| \leq \left(\frac{35 + 13\sqrt{13}}{216}\right)^{1/3} D_F^{1/3} \quad \text{and} \quad |\omega_3| \leq \frac{4}{27}D_F^{1/2},$$

whence, after a little computation, we find that

$$|\omega_0| + |\omega_1| + |\omega_2| + |\omega_3| < D_F^{1/2} = 2p^{1/2}.$$

From (42), it follows that

$$|\alpha_1| \leq |\omega_0| + |\omega_1| + |\omega_2| + |\omega_3| < 2p^{1/2},$$

whereby inequalities (49) and (40) thus yield

$$|u/v| < 2p^{1/2} + 0.12 < 2^{23.1},$$

and so, again appealing to (40), $\min\{|u|, |v|\} > 2^{104}$. Returning to inequality (47), we find that, after applying (44),

$$|H_F(\alpha_1, 1) - H_F(u/v, 1)| \leq 2p^{1/2}\left(4p^{1/2} + 1.24\right)2^{7/3}(2p)^{-1/6}v^{-2}.$$

From $p < 2 \times 10^{13}$ and $|v| > 2^{104}$, it follows that

$$|H_F(\alpha_1, 1) - H_F(u/v, 1)| < 10^{-50}.$$

Combining this with (44) and (45) yields the inequality

$$|H_F(u/v, 1)| > \frac{2p}{|\omega_1^2 - 3\omega_0\omega_2|},$$

whence

$$|H_F(u, v)| = v^2\,|H_F(u/v, 1)| > \frac{2v^2p}{|\omega_1^2 - 3\omega_0\omega_2|} \geq v^2\sqrt{p},$$

where the last inequality follows from (44). From (40) and the fact that $|v| > 2^{104}$, we conclude that

$$|H_F(u,v)| > 10^{67}.$$

Next, suppose that F has negative discriminant, so that H_F has positive discriminant $D_{H_F} = -3D_F$. If $\omega_1^2 - 3\omega_0\omega_2 = 0$, then, from (43), we have that

$$3p = -(\omega_1^2 - 3\omega_0\omega_2)(\omega_2^2 - 3\omega_1\omega_3),$$

which implies that

$$\max\left\{|\omega_1^2 - 3\omega_0\omega_2|, |\omega_2^2 - 3\omega_1\omega_3|\right\} \geq p.$$

On the other hand, from Lemma 6.4 of Belabas and Cohen [4], we have

$$\begin{gathered} |\omega_0| \leq \tfrac{2^{3/2}p^{1/4}}{3^{3/4}},\ |\omega_1| \leq \tfrac{2^{3/2}p^{1/4}}{3^{1/4}},\ \max\{|\omega_0\omega_2^3|, |\omega_1^3\omega_3|\} \leq \tfrac{(11+5\sqrt{5})p}{2}, \\ |\omega_1\omega_2| \leq \tfrac{8p^{1/2}}{3^{1/2}} \ \text{ and } \ |\omega_0\omega_3| \leq \tfrac{2p^{1/2}}{3^{1/2}}, \end{gathered} \tag{50}$$

whereby a short calculation, together with the fact that $p > 2 \times 10^9$, yields a contradiction. We may thus suppose that $\omega_1^2 - 3\omega_0\omega_2 \neq 0$. We have

$$H_F(\alpha_i, 1) = (\omega_1^2 - 3\omega_0\omega_2)\,(\alpha_i - \beta_1)\,(\alpha_i - \beta_2)\,,$$

where

$$\beta_j = \frac{9\omega_0\omega_3 - \omega_1\omega_2 + (-1)^j\sqrt{12p}}{2(\omega_1^2 - 3\omega_0\omega_2)} \quad \text{for} \quad j \in \{1,2\}.$$

It follows that

$$|\beta_j| \leq |\omega_1^2 - 3\omega_0\omega_2|^{-1} 44 \cdot 3^{-1/2} p^{1/2}$$

and, again from (42),

$$|\omega_0\alpha_i| \leq |\omega_0| + |\omega_1| + |\omega_2| + |\omega_3|,$$

whereby

$$|\omega_0\alpha_i| \leq \frac{2^{3/2}p^{1/4}}{3^{3/4}} + \frac{2^{3/2}p^{1/4}}{3^{1/4}} + \frac{2^{2/3}\left(11+5\sqrt{5}\right)^{1/3}p^{1/2}}{3^{1/2}|\omega_0|} + \frac{2p^{1/2}}{3^{1/2}|\omega_0|},$$

whence we find that

$$|\alpha_i| \leq \frac{3.4\,p^{1/4}}{|\omega_0|} + \frac{2.1\,p^{1/2}}{|\omega_0|^2} < \frac{6.4\,p^{1/2}}{|\omega_0|^2}.$$

From (41), we thus have

$$|H_F(\alpha_1, 1)| \geq \omega_0^{-2}(\omega_1^2 - 3\omega_0\omega_2)^{-2} \min\left\{\frac{\omega_0^2}{3.2}, \frac{|\omega_1^2 - 3\omega_0\omega_2|}{12.8}\right\}^2.$$

If $|\omega_1^2 - 3\omega_0\omega_2| > 4\omega_0^2$, it follows that

$$|H_F(\alpha_1, 1)| \geq \frac{\omega_0^2}{10.24\,(\omega_1^2 - 3\omega_0\omega_2)^2}$$

and so

$$|H_F(\alpha_1, 1)| \geq \frac{1}{10.24\,(2^3 3^{-1/2}p^{1/2} + 2^{2/3}3^{1/2}\left(11+5\sqrt{5}\right)^{1/3}p^{1/2})^2}$$

which implies that

$$|H_F(\alpha_1, 1)| > \frac{1}{1561\,p}. \tag{51}$$

If, conversely, $|\omega_1^2 - 3\omega_0\omega_2| \leq 4\omega_0^2$, then

$$|H_F(\alpha_1, 1)| \geq \frac{1}{163.84\,\omega_0^2} > \frac{1}{253\sqrt{p}}$$

and hence (51) holds in either case.

Now, if $\alpha_1 \notin \mathbb{R}$, then, via Mahler [41],

$$|\mathrm{Im}(\alpha_1)| \geq \frac{1}{18}\left(|\omega_0| + |\omega_1| + |\omega_2| + |\omega_3|\right)^{-2} > \frac{\omega_0^2}{738\,p},$$

so that

$$\left|\alpha_1 - \frac{u}{v}\right| > \frac{\omega_0^2}{738\,p}$$

and hence

$$8 = |\omega_0||v|^3 \left|\alpha_1 - \frac{u}{v}\right| \left|\alpha_2 - \frac{u}{v}\right| \left|\alpha_3 - \frac{u}{v}\right| > |\omega_0||v|^3 \left(\frac{\omega_0^2}{738\,p}\right)^3.$$

It follows that

$$|v| < 1476p < 2.952 \times 10^{16},$$

via (40). Since $\max\{|u|, |v|\} > 2^{128}$, we thus have

$$|u/v| > 1.15 \times 10^{22}.$$

From

$$|\alpha_1| < 6.4p^{1/2} < 6.4\left(2 \times 10^{13}\right)^{1/2} < 3 \times 10^7,$$

we may thus conclude that

$$\left|\alpha_1 - \frac{u}{v}\right| > 1.14 \times 10^{22}$$

and so

$$8 \geq \left(1.14 \times 10^{22}\right)^3,$$

an immediate contradiction.

We may thus suppose that $\alpha_1 \in \mathbb{R}$ (so that $\alpha_2, \alpha_3 \notin \mathbb{R}$). It follows from Mahler [41] that

$$\left|\alpha_i - \frac{u}{v}\right| > \frac{\omega_0^2}{738\,p} \quad \text{for} \quad i \in \{2, 3\},$$

and so

$$\left|\alpha_1 - \frac{u}{v}\right| < \frac{8}{|\omega_0||v|^3}\left(\frac{738p}{\omega_0^2}\right)^2. \tag{52}$$

Appealing to (40) and the inequalities $|\alpha_1| < 3 \times 10^7$ and $|v| \geq 1$, we thus have that

$$|u/v| < 1.75 \times 10^{33} + 3 \times 10^7 < 1.76 \times 10^{33},$$

and so, from $\max\{|u|, |v|\} > 2^{128}$, $|v| > 1.9 \times 10^5$. Inequality (52) thus now implies

$$|u/v| < 2.6 \times 10^{17},$$

whence $|v| > 1.3 \times 10^{21}$. Substituting this a third time into (52),

$$\left|\alpha_1 - \frac{u}{v}\right| < 10^{-30},$$

so that $|u/v| < 3.1 \times 10^7$ and $|v| > 10^{31}$. One final use of (52) thus yields the inequality

$$\left|\alpha_1 - \frac{u}{v}\right| < 10^{-59}.$$

Appealing to (40), (46), (50), and the fact that $|\alpha_1| < 3 \times 10^7$, we thus have, after a little work,

$$|H_F(\alpha_1, 1) - H_F(u/v, 1)| < 3.4 \times 10^{-44}.$$

With (51), this implies that

$$|H_F(u/v, 1)| > \frac{1}{1562\, p}$$

and so

$$|H_F(u, v)| = v^2\, |H_F(u/v, 1)| > \frac{v^2}{1562p} > \frac{10^{62}}{3124 \times 10^{13}} > 3 \times 10^{45},$$

as claimed. □

11. Concluding remarks

Many of the techniques of this paper can be generalized to potentially treat the problem of determining elliptic curves of a given conductor over a number field K. In case K is an imaginary quadratic field of class number 1, then, in fact, such an approach works without any especially new ingredients. We will discuss this in subsequent work.

Acknowledgments

The authors are extremely grateful to the referees for numerous helpful comments that improved both the exposition and, more importantly, the mathematical correctness of the paper.

References

[1] M. K. Agrawal, J. H. Coates, D. C. Hunt, and A. J. van der Poorten, *Elliptic curves of conductor* 11, Math. Comp. **35** (1980), no. 151, 991–1002, DOI 10.2307/2006209. MR572871

[2] S. Akhtari and M. Bhargava, *A positive proportion of locally soluble Thue equations are globally insoluble*, preprint. Amer. J. Math., to appear.

[3] K. Belabas, *A fast algorithm to compute cubic fields*, Math. Comp. **66** (1997), no. 219, 1213–1237, DOI 10.1090/S0025-5718-97-00846-6. MR1415795

[4] K. Belabas and H. Cohen, *Binary cubic forms and cubic number fields*, Organic mathematics (Burnaby, BC, 1995), CMS Conf. Proc., vol. 20, Amer. Math. Soc., Providence, RI, 1997, pp. 175–204. MR1483919

[5] M. A. Bennett and A. Ghadermarzi, *Mordell's equation: a classical approach*, LMS J. Comput. Math. **18** (2015), no. 1, 633–646, DOI 10.1112/S1461157015000182. MR3406453

[6] M. A. Bennett and A. Rechnitzer, *Computing elliptic curves over* $\mathbb{Q}$ *: bad reduction at one prime*, CAIMS 2015 proceedings.

[7] L. Bernardin et al, *Maple Programming Guide*, Maplesoft, 2017, Waterloo ON, Canada.

[8] B. J. Birch and W. Kuyk (eds.), *Modular Functions of One Variable. IV*, Lecture Notes in Mathematics, Vol. 476, Springer-Verlag, Berlin-New York, 1975. MR0376533

[9] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, Computational algebra and number theory (London, 1993), J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. MR1484478

[10] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939, DOI 10.1090/S0894-0347-01-00370-8. MR1839918

[11] A. Brumer and O. McGuinness, *The behavior of the Mordell-Weil group of elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 375–382, DOI 10.1090/S0273-0979-1990-15937-3. MR1044170

[12] A. Brumer and J. H. Silverman, *The number of elliptic curves over* $\mathbf{Q}$ *with conductor* N, Manuscripta Math. **91** (1996), no. 1, 95–102, DOI 10.1007/BF02567942. MR1404420

[13] J. Coates, *An effective p-adic analogue of a theorem of Thue. III. The diophantine equation* $y^2 = x^3 + k$, Acta Arith. **16** (1969/1970), 425–435, DOI 10.4064/aa-16-4-425-436. MR0263742
[14] F. Coghlan, *Elliptic Curves with Conductor* $2^m 3^n$, Ph.D. thesis, Manchester, England, 1967.
[15] J. E. Cremona, *Elliptic curve tables*, `http://johncremona.github.io/ecdata/`
[16] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd ed., Cambridge University Press, Cambridge, 1997. MR1628193
[17] J. E. Cremona, *Reduction of binary cubic and quartic forms*, LMS J. Comput. Math. **2** (1999), 64–94, DOI 10.1112/S1461157000000073. MR1693411
[18] J. E. Cremona, *mwrank and related programs for elliptic curves over* $\mathbb{Q}$, 1990–2017, `http://www.warwick.ac.uk/staff/J.E.Cremona/mwrank/index.html`
[19] J. E. Cremona and M. P. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Experiment. Math. **16** (2007), no. 3, 303–312. MR2367320
[20] H. Davenport, *The reduction of a binary cubic form. I*, J. London Math. Soc. **20** (1945), 14–22, DOI 10.1112/jlms/s1-20.1.14. MR0015432
[21] H. Davenport, *The reduction of a binary cubic form. II*, J. London Math. Soc. **20** (1945), 139–147, DOI 10.1112/jlms/s1-20.3.139. MR0015433
[22] H. Davenport, *On the class-number of binary cubic forms. I*, J. London Math. Soc. **26** (1951), 183–192, DOI 10.1112/jlms/s1-26.3.183. MR0043822
[23] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420, DOI 10.1098/rspa.1971.0075. MR0491593
[24] B. Edixhoven, A. de Groot, and J. Top, *Elliptic curves over the rationals with bad reduction at only one prime*, Math. Comp. **54** (1990), no. 189, 413–419, DOI 10.2307/2008702. MR995209
[25] N. D. Elkies, *How many elliptic curves can have the same prime conductor?*, `http://math.harvard.edu/~elkies/condp_banff.pdf`
[26] N. D. Elkies, *Rational points near curves and small nonzero* $|x^3 - y^2|$ *via lattice reduction*, Algorithmic number theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 33–63, DOI 10.1007/10722028_2. MR1850598
[27] N. D. Elkies and M. Watkins, *Elliptic curves of large rank and small conductor*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 42–56, DOI 10.1007/978-3-540-24847-7_3. MR2137342
[28] A. Gherga, *Implementation of a Thue-Mahler solver and related problems*, Ph.D. thesis, University of British Columbia, 2018.
[29] T. Hadano, *On the conductor of an elliptic curve with a rational point of order* 2, Nagoya Math. J. **53** (1974), 199–210. MR0354673
[30] B. Haible, *CLN, a class library for numbers*, available from `http://www.ginac.de/CLN/`
[31] K. Hambrook, *Implementation of a Thue-Mahler solver*, M.Sc. thesis, University of British Columbia, 2011.
[32] H. Hasse, *Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage* (German), Math. Z. **31** (1930), no. 1, 565–582, DOI 10.1007/BF01246435. MR1545136
[33] C. Hermite, *Note sur la réduction des fonctions homogènes à coefficients entiers et à deux indéterminées* (French), J. Reine Angew. Math. **36** (1848), 357–364, DOI 10.1515/crll.1848.36.357. MR1578622
[34] C. Hermite, *Sur la réduction des formes cubiques à deux indéterminées*, C. R. Acad. Sci. Paris 48 (1859), 351–357.
[35] G. Julia, *Étude sur les formes binaires non quadratiques à indéterminées réelles, ou complexes, ou à indéterminées conjuguées* (French), NUMDAM, [place of publication not identified], 1917. MR3532882
[36] R. von Kanel and B. Matschke, *Solving S-unit, Mordell, Thue, Thue-Mahler and generalized Ramanujan-Nagell equations via Shimura-Taniyama conjecture*, preprint, arXiv:1605.06079.
[37] A. Koutsianas, *Computing all elliptic curves over an arbitrary number field with prescribed primes of bad reduction*, Experiment. Math., `http://www.tandfonline.com/doi/full/10.1080/10586458.2017.1325791`
[38] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, http://www.lmfdb.org
[39] K. Mahler, *Zur Approximation algebraischer Zahlen. I* (German), Math. Ann. **107** (1933), no. 1, 691–730, DOI 10.1007/BF01448915. MR1512822

[40] K. Mahler, *An application of Jensen's formula to polynomials*, Mathematika **7** (1960), 98–100, DOI 10.1112/S0025579300001637. MR0124467
[41] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. **11** (1964), 257–262. MR0166188
[42] G. B. Mathews and W. E. H. Berwick, *On the reduction of arithmetical binary cubics which have a negative determinant*, Proc. London Math. Soc. (2) **10** (1912), 48–53, DOI 10.1112/plms/s2-10.1.48. MR1576036
[43] J.-F. Mestre and J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance m-ième* (French), J. Reine Angew. Math. **400** (1989), 173–184, DOI 10.1515/crll.1989.400.173. MR1013729
[44] G. L. Miller, *Riemann's hypothesis and tests for primality*, Seventh Annual ACM Symposium on Theory of Computing (Albuquerque, N.M., 1975), Assoc. Comput. Mach., New York, 1975, pp. 234–239. MR0480296
[45] L. J. Mordell, *The Diophantine Equation* $y2 - k = x3$, Proc. London Math. Soc. (2) **13** (1914), 60–80, DOI 10.1112/plms/s2-13.1.60. MR1577519
[46] L. J. Mordell, *Diophantine equations*, Pure and Applied Mathematics, Vol. 30, Academic Press, London-New York, 1969. MR0249355
[47] T. Nagell, *Introduction to Number Theory*, John Wiley & Sons, Inc., New York; Almqvist & Wiksell, Stockholm, 1951. MR0043111
[48] O. Neumann, *Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. II* (German), Math. Nachr. **56** (1973), 269–280, DOI 10.1002/mana.19730560127. MR0338000
[49] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle* 2 *et* 3, J. Number Theory **44** (1993), no. 2, 119–152, DOI 10.1006/jnth.1993.1040. MR1225948
[50] The PARI Group, Bordeaux. PARI/GP version `2.7.1`, 2014, available at `http://pari.math.u-bordeaux.fr/`.
[51] J. Park, B. Poonen, J. Voight and M. Matchett Wood, *A heuristic for boundedness of ranks of elliptic curves*, preprint, arXiv:1602.01431.
[52] A. Pethő, *On the resolution of Thue inequalities*, J. Symbolic Comput. **4** (1987), no. 1, 103–109, DOI 10.1016/S0747-7171(87)80059-7. MR908418
[53] A. Pethő, *On the representation of* 1 *by binary cubic forms with positive discriminant*, Number theory (Ulm, 1987), Lecture Notes in Math., vol. 1380, Springer, New York, 1989, pp. 185–196, DOI 10.1007/BFb0086553. MR1009801
[54] M. O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory **12** (1980), no. 1, 128–138, DOI 10.1016/0022-314X(80)90084-0. MR566880
[55] K. Rubin and A. Silverberg, *Mod* 2 *representations of elliptic curves*, Proc. Amer. Math. Soc. **129** (2001), no. 1, 53–57, DOI 10.1090/S0002-9939-00-05539-8. MR1694877
[56] The Sage Developers, SageMath, the Sage Mathematics Software System (Version 8.1), `http://www.sagemath.org`, 2018.
[57] B. Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. (2) **10** (1975), 367–378, DOI 10.1112/jlms/s2-10.3.367. MR0371904
[58] I. R. Šafarevič, *Algebraic number fields* (Russian), Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 163–176. MR0202709
[59] D. Shanks, *Five number-theoretic algorithms*, Proceedings of the Second Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1972), Utilitas Math., Winnipeg, Man., 1973, pp. 51–70. Congressus Numerantium, No. VII. MR0371855
[60] A. K. Silvester, B. K. Spearman, and K. S. Williams, *Cyclic cubic fields of given conductor and given index*, Canad. Math. Bull. **49** (2006), no. 3, 472–480, DOI 10.4153/CMB-2006-046-1. MR2252268
[61] J. Sorenson and J. Webster, *Strong pseudoprimes to twelve prime bases*, Math. Comp. **86** (2017), no. 304, 985–1003, DOI 10.1090/mcom/3134. MR3584557
[62] V. G. Sprindžuk, *Classical Diophantine Equations*, Lecture Notes in Mathematics, vol. 1559, Springer-Verlag, Berlin, 1993. MR1288309
[63] W. A. Stein and M. Watkins, *A database of elliptic curves—first report*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 267–275, DOI 10.1007/3-540-45455-1_22. MR2041090
[64] N. M. Stephens, *The Birch Swinnerton-Dyer Conjecture for Selmer curves of positive rank*, Ph.D. Thesis, Manchester, 1965.

[65] O. Tange, *GNU Parallel - The Command-Line Power Tool*, ;login: The USENIX Magazine, (2011), 42–47.
[66] A. Thue, *Über Annäherungswerte algebraischer Zahlen* (German), J. Reine Angew. Math. **135** (1909), 284–305, DOI 10.1515/crll.1909.135.284. MR1580770
[67] N. Tzanakis and B. M. M. de Weger, *On the practical solution of the Thue equation*, J. Number Theory **31** (1989), no. 2, 99–132, DOI 10.1016/0022-314X(89)90014-0. MR987566
[68] N. Tzanakis and B. M. M. de Weger, *Solving a specific Thue-Mahler equation*, Math. Comp. **57** (1991), no. 196, 799–815, DOI 10.2307/2938718. MR1094961
[69] N. Tzanakis and B. M. M. de Weger, *How to explicitly solve a Thue-Mahler equation*, Compositio Math. **84** (1992), no. 3, 223–288. MR1189890
[70] M. Watkins, S. Donnelly, N. D. Elkies, T. Fisher, A. Granville, and N. F. Rogers, *Ranks of quadratic twists of elliptic curves*, Numéro consacré au trimestre "Méthodes arithmétiques et applications", automne 2013, Publ. Math. Besançon Algèbre Théorie Nr., vol. 2014/2, Presses Univ. Franche-Comté, Besançon, 2015, pp. 63–98. MR3381037
[71] B. M. M. de Weger, *Algorithms for Diophantine equations*, CWI Tract, vol. 65, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 1989. MR1026936
[72] B. M. M. de Weger, *The weighted sum of two S-units being a square*, Indag. Math. (N.S.) **1** (1990), no. 2, 243–262, DOI 10.1016/0019-3577(90)90007-A. MR1060828
[73] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551, DOI 10.2307/2118559. MR1333035

Department of Mathematics, University of British Columbia, Vancouver, British Columbia, Canada
Email address: bennett@math.ubc.ca

Department of Mathematics, University of British Columbia, Vancouver, British Columbia, Canada
Email address: ghergaa@math.ubc.ca

Department of Mathematics, University of British Columbia, Vancouver, British Columbia, Canada
Email address: andrewr@math.ubc.ca