COMPUTING ELLIPTIC CURVES OVER $\mathbb{Q}$: BAD REDUCTION AT ONE PRIME

MICHAEL A. BENNETT AND ANDREW RECHNITZER

Abstract. We discuss a new algorithm for finding all elliptic curves over $\mathbb{Q}$ with a given conductor. Though based on (very) classical ideas, this approach appears to be computationally quite efficient. We provide details of the output from the algorithm in case of conductor p or p^2, for p prime, with comparisons to existing data.

1. Introduction

Elliptic curves are ubiquitous objects in pure mathematics, particularly in Number Theory and Algebraic Geometry, but, in recent years, they also have found their way into an increasing numbers of applications, ranging from primality testing to factoring, and are the basis for a commonly used public-key cryptosystem. It is therefore of some interest to be able to generate or tabulate elliptic curves with desired properties. In this paper, we will describe an algorithm for computing models for all elliptic curves with integer coefficients and bounded *conductor*. This last quantity is an invariant that provides information about how a given elliptic curve behaves over finite fields $\mathbb{F}_p$, as p ranges over all primes.

If K is a number field and S is a finite set of places of K, containing the infinite places, then a theorem of Shafarevich [39] from 1963 ensures that there are at most finitely many K-isomorphism classes of elliptic curves defined over K with good reduction outside S. In the simplest case, where $K = \mathbb{Q}$, an effective version of this result was proved by Coates [11] in 1970, using bounds for linear forms in p-adic and complex logarithms. Early attempts to make such results explicit, for fixed sets of "small" primes S, have much in common with the arguments of ([11]), in that they (often) reduce the problem to one of solving a number of *Thue-Mahler equations*. These are Diophantine equations of the form

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

where F is a binary form (of degree at least 3) and u is an *S-unit*, that is, an integer whose prime factors all lie in S (strictly speaking, for $K = \mathbb{Q}$, we are assuming here that $2 \in S$). In case the form F is reducible in $\mathbb{Z}[x, y]$ (which turns out to be the case when the elliptic curves we are considering have at least one rational 2-torsion point), equation (1) typically is somewhat less challenging to solve. The earliest examples where a complete determination of all elliptic curves $E/\mathbb{Q}$ with good reduction outside a given set S was made were for $S = \{2, 3\}$ (by Coghlan

Date: November 26, 2015.

1991 *Mathematics Subject Classification.* Primary 11G05, 11D25, 11D59, Secondary 11E76, 11Y50, 11Y65.

Key words and phrases. elliptic curves, cubic forms, invariant theory.

The authors were supported in part by grants from NSERC.

[12] and Stevens (see e.g. [7])), and for $S = \{p\}$ for certain small primes p (by e.g. Setzer [38] and Neumann [33]).

The first case where such a determination was made with corresponding forms in equation (1) irreducible was for $S = \{11\}$, by Agrawal, Coates, Hunt and van der Poorten [1]. The reduction to (1) in this situation is not especially problematical, but subsequent computations (involving the arguments of [11] together with a variety of techniques from computational Diophantine approximation) are quite involved. For whatever reason, there are very few if any subsequent attempts in the literature to find elliptic curves of given conductor via Thue-Mahler equations. Instead, one finds a wealth of results on a completely different approach to the problem, using modular forms. This method relies upon the Modularity theorem of Breuil, Conrad, Diamond and Taylor [8], which was still a conjecture (under various guises) when these ideas were first implemented. Much of the success of this approach can be attributed to Cremona (see e.g. [13], [14]) and his collaborators, who have devoted decades of work to it (and are responsible for the current state-of-the-art). To apply this method to find all $E/\mathbb{Q}$ of conductor N, 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 [14]. Via this method (assuming the results of [8]), all $E/\mathbb{Q}$ of conductor N were determined for values of N as follows.

- Antwerp IV (1972) $N \leq 200$
- Tingley (1975) $N \leq 320$
- Cremona (1988) $N \leq 600$
- Cremona (1990) $N \leq 1000$
- Cremona (1997) $N \leq 5077$
- Cremona (2001) $N \leq 10000$
- Cremona (2005) $N \leq 130000$
- Cremona (2014) $N \leq 350000$
- Cremona (2015) $N \leq 364000$

In this paper, we will instead return to techniques based upon solving Thue-Mahler equations. Our goal is to provide a treatment that makes the connection between the conductors in question and the corresponding equations (1) straightforward, and the subsequent Diophantine approximation problem as painless as possible. We will rely upon a number of results from classical invariant theory. The outline of our paper is as follows. In Section 2, we will outline some basic facts and notation about elliptic curves. In Section 3, we will discuss the invariant theory of cubic forms and state our main theorem which provides our algorithm. Section 4 is devoted to the actual computation of the cubic forms we require. In Section 5, we discuss the special cases where $N = p$ or p^2 for p prime while, in Section 6, we provide a variety of computational details for these cases and an outline of a heuristic approach to the problem. Finally, in Section 7, we give an overview of our output, comparing it to previous results in the literature. We should note that this paper is an abridged version of forthcoming work of the authors [5]. Readers interested in the proofs of a number of results stated here as well as more extensive data should consult that paper.

2. Elliptic curves

Let $S = \{p_1, p_2, \ldots, p_k\}$ be a set of rational primes. Suppose that we wish to find models for isomorphism classes of elliptic curve over $\mathbb{Q}$ with given conductor $N = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where the α_i are positive integers. Such a curve has a minimal model

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

with the $a_i \in \mathbb{Z}$ and discriminant $\Delta_E = (-1)^\delta p_1^{\beta_1} \cdots p_k^{\beta_k}$, where the $\beta_i \geq \alpha_i$ are again positive integers and $\delta \in \{0, 1\}$. Writing

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

$$c_4 = b_2^2 - 24b_4 \ \text{ and } \ c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$$

we find that

$$1728\Delta_E = c_4^3 - c_6^2$$

and

$$j_E = c_4^3/\Delta_E.$$

We therefore have

$$c_6^2 = c_4^3 + (-1)^{\delta+1}L, \tag{2}$$

where

$$L = 2^6 \cdot 3^3 \cdot p_1^{\beta_1} \cdots p_k^{\beta_k}.$$

For each prime p, since our model is minimal, we may suppose (via Tate's algorithm; see e.g. Papadopolous [34]), defining $\nu_p(x)$ to be the largest power of a prime p dividing a nonzero integer x, that

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

In fact, it is equation (2) that lies at the heart of our approach (see also Cremona and Lingham [16] for an approach to the problem that takes as its starting point equation (2), but then heads in a rather different direction).

3. Cubic forms

Let us suppose that a, b, c and d are integers, and consider the binary cubic form

$$F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3, \tag{4}$$

with discriminant

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

To such a form we associate a pair of covariants, the Hessian $H = H_F(x, y)$ given by

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

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

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

Note that, explicitly,

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

and

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

These covariants satisfy the syzygy

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

We further have

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

We can now state our main result, which leads to our algorithm.

Theorem 3.1. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N = 2^\alpha 3^\beta N_0$, where N_0 is coprime to 6. Then there exists an integral binary cubic form F of discriminant*

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

and relatively prime integers u and v with

$$F(u,v) = \omega_0 u^3 + \omega_1 u^2 v + \omega_2 u v^2 + \omega_3 v^3 = 2^{\alpha_1}\cdot 3^{\beta_1}\cdot \prod_{p\mid N_0} p^{\kappa_p}. \tag{6}$$

Here, $N_1 \mid N_0$,

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

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

and $\kappa_p \in \mathbb{Z}$ with $\kappa_p \in \{0,1\}$ if $p^2 \mid K$. If $\beta_0 \geq 3$, we further have that $3 \mid \omega_1$ and $3 \mid \omega_2$. Writing

$$\mathcal{D} = \prod_{p\mid \gcd(c_4(E),c_6(E))} p^{\min\{[\nu_p(c_4(E))/2],[\nu_p(c_6(E))/3]\}} \tag{7}$$

and

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

it follows that E is isomorphic over $\mathbb{Q}$ to $E_{\mathcal{D}}$.

A few observations are worth making here. Firstly, the above conditions are not sufficient in the sense that there might exists such a form and corresponding $E_{\mathcal{D}}$, but we might have that the conductor $N_{E_{\mathcal{D}}} \neq N$ (this can occur if certain local conditions at 2 are not satisfied). It is also the case, that the cubic forms arising need not be either primitive (in the sense that $\gcd(\omega_0,\omega_1,\omega_2,\omega_3) = 1$) or irreducible. The former situation (i.e. that of imprimitive forms) can occur if each of the coefficients of F is divisible by 3. The latter occurs precisely when the

curve E has at least one rational 2-torsion point. It is also worth noting here that necessarily

$$\mathcal{D} \mid 2^3 \cdot 3^2 \cdot \prod_{p \mid N_0} p. \tag{8}$$

In the event that, for a given binary form $F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, we have $3 \mid b$ and $3 \mid c$, say $b = 3b_0$ and $c = 3c_0$, then we have that $27 \mid D_F$ and 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 may observe that the set of forms with both $3 \mid b$ and $3 \mid c$ is closed within the larger set of all binary cubic forms in $\mathbb{Z}[x,y]$, under the action of both $\mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z})$. Note that, for such a form, 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

$$\begin{aligned}\widetilde{G}_F(x,y) = \tfrac{G_F(x,y)}{27} = (&-a^2d + 3ab_0c_0 - 2b_0^3)x^3 + 3(-b_0^2c_0 - ab_0d + 2ac_0^2)x^2y \\ &+3(b_0c_0^2 - 2b_0^2d + ac_0d)xy^2 + (-3b_0c_0d + 2c_0^3 + ad^2)y^3,\end{aligned}$$

whereby our syzygy now becomes

$$4\widetilde{H}_F(x,y)^3 = \widetilde{G}_F(x,y)^2 + \widetilde{D}_F F(x,y)^2. \tag{9}$$

Theorem 3.1 is essentially a slight generalization of a very classical result of Mordell [31] (see also Theorem 3 of Chapter 24 of Mordell [32]), where 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 could be eliminated, with some care, was noted by Sprindzuk (see Chapter VI of [41]).

Converting Theorem 3.1 into an algorithm for finding all $E/\mathbb{Q}$ of conductor N is a straightforward exercise. We proceed as follows.

(1) 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) give in the statement of Theorem 3.1. The (very efficient) algorithm for carrying this out is described in detail in Section 4.

(2) Solve the corresponding Thue-Mahler equations. This is a deterministic procedure (see Tzanakis and de Weger [45], [46]) but not, in general, one that could reasonably be described as routine.

(3) Check "local" conditions and output the elliptic curves that arise.

As we shall see, the first and third of these steps are straightforward (indeed, the third is essentially trivial). All of the real work is concentrated in step (2). In Section 5, we will focus our attention on carrying out this procedure in the special case where $N = p$ or $N = p^2$ for p prime. For these conductors, we encounter the happy circumstance that the Thue-Mahler equations (6) reduce to Thue equations (i.e. where the exponents on the right hand side of (6) are all absolutely bounded).

In such a situation, there are easily implemented computational routines for solving such equations, available in Pari/GP or in Magma. Further, it is possible to apply a much more computationally efficient argument to find all such elliptic curves heuristically (but not deterministically). We will describe such an approach later in the paper, in Section 6.

4. Finding representative forms

As we have seen, in order to find elliptic curves over $\mathbb{Q}$ with good reduction outside a given set of primes, it suffices to determine a set of representatives for $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of binary cubic forms with certain discriminants, and then solve a number of corresponding Thue-Mahler equations. In this section, we will describe how to find distinguished *reduced* representatives for equivalence classes of cubic forms with a given discriminant. In each case, the notion of *reduction* is related to associating to a given cubic form a particular definite quadratic form – in case of positive discriminant, for example, the Hessian H defined earlier. In what follows, we will state our definitions of reduction solely in terms of the coefficients of the given cubic form, keeping the associated Hessian hidden.

4.1. **Forms of positive discriminant.** In the case of positive discriminant forms, we will appeal to a classical reduction theory, dating back to work of Hermite [26], [27] and later used by Davenport (see e.g. [17], [18] and [19]). This procedure allows us to determine a *reduced* element within a given equivalence class of forms. We will assume the forms we are treating are irreducible, (and treat the case of reducible forms somewhat differently). We follow work of Belabas [2] (see also Belabas and Cohen [3] and Cremona [15]), a modern treatment and refinement of Hermite's method.

Definition 1. *An irreducible binary integral cubic form*

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

of positive discriminant is called reduced if we have

- $|bc - 9ad| \leq b^2 - 3ac \leq c^2 - 3bd$,
- $a > 0, b \geq 0$, *where* $d < 0$ *whenever* $b = 0$,
- *if* $bc = 9ad, d < 0$,
- *if* $b^2 - 3ac = bc - 9ad$, $b < |3a - b|$, *and*
- *if* $b^2 - 3ac = c^2 - 3bd$, $a \leq |d|$, *and* $b < |c|$ *whenever* $|d| = a$.

The main value of this notion of reduction is in the following result (Corollary 3.3 of [2]).

Proposition 4.1. *Any irreducible cubic form with positive discriminant is* $GL_2(\mathbb{Z})$*-equivalent to a unique reduced one.*

To determine equivalence classes of reduced cubic forms with bounded discriminant, we will appeal to the following result (Lemma 3.5 of Belabas [2]).

Lemma 4.2. *Let* X *be a positive real number and*

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

be a reduced form whose discriminant lies in $(0, X]$. *Then we have*

$$1 \leq a \leq \frac{2X^{1/4}}{3\sqrt{3}}$$

and

$$0 \leq b \leq \frac{3a}{2} + \left(\sqrt{X} - \frac{27a^2}{4}\right)^{1/2}.$$

If we denote by P_2 the unique positive real solution of the equation

$$-4P_2^3 + (3a+2b)^2 P_2^2 + 27a^2 Z = 0,$$

then

$$\frac{b^2 - P_2}{3a} \leq c \leq b - 3a.$$

4.2. **Forms of negative discriminant.** In case of negative discriminant, we require a different notion of reduction, as the Hessian is no longer a definite form. We will instead, following Belabas [2], use an idea of Berwick and Mathews [6]. We take as our definition of a reduced form an alternative characterization due to Belabas (Lemma 4.2 of [2]).

Definition 2. *An irreducible binary integral cubic form*

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

of negative discriminant is called reduced if we have

- $d^2 - a^2 > bd - ac$,
- $-(a-b)^2 - ac < ad - bc < (a+b)^2 + ac$,
- $a > 0$, $b \geq 0$ *and* $d > 0$ *whenever* $b = 0$.

Analogous to Proposition 4.1, we have, as a consequence of Lemma 4.3 of [2] :

Proposition 4.3. *Any irreducible cubic form with negative discriminant is $GL_2(\mathbb{Z})$-equivalent to a unique reduced one.*

To count the number of reduced cubic forms in this case, we use Lemma 4.4 of Belabas [2] :

Lemma 4.4. *Let X be a positive real number and*

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

be a reduced form whose discriminant lies in $[-X, 0)$. Then we have

$$1 \leq a \leq \left(\frac{16X}{27}\right)^{1/4}$$

$$0 \leq b \leq \frac{3a}{2} + \left(\sqrt{X/3} - \frac{3a^2}{4}\right)^{1/2}$$

$$1 - b \leq c \leq \left(\frac{X}{4a}\right)^{1/3} + \begin{cases} b^2/3a & \text{if } a \geq 2b/3, \\ b - 3a/4 & \text{otherwise.} \end{cases}$$

It is worth noting here that a different notion of reduction for cubic forms of negative discriminant is described in Cremona [15], arising from classical work of Julia [28]. This definition leads to shorter loops for the coefficient a and a slight improvement in the expected complexity (though the number of (a,b,c,d) one treats still grows linearly in the variable X).

4.3. **Reducible forms.** We can define somewhat similar notions of reduction for reducible forms (see e.g. [4]). For our purposes, though, it is enough to recall that we may suppose that a reduced form is equivalent to one of the shape

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

whereby we have

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

To determine all elliptic curves with good reduction outside $S = \{p_1, p_2, \ldots, p_k\}$, corresponding to reducible cubics in Theorem 3.1 (i.e. those E with at least one rational 2-torsion point), it suffices to find all such triples (b, c, d) for which there exists integers x and y with, writing $S^* = S \cup \{2\}$, both $b^2(c^2 - 4bd)$ and $bx^2y + cxy^2 + dy^3$ S^*-units. For this to occur, it is clearly necessary that $b, c^2 - 4bd, y$ and $\mu = bx^2 + cxy + dy^2$ are S^*-units. Taking the discriminant of this last quadratic as a function of x, we thus require that

$$(c^2 - 4bd)y^2 + 4b\mu = Z^2, \tag{10}$$

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

$$X + Y = Z^2 \tag{11}$$

in S^*-units X and Y. There is an algorithm for solving such equations described in detail in Chapter 7 of de Weger [48] (see also [49]), relying upon bounds for linear forms in p-adic and complex logarithms and various reduction techniques. While *a priori* equation (10) arises as only a necessary condition for the existence of an elliptic curve of the desired form, given any solution to (10), the curve

$$E \ : \ y^2 = x^3 + Zx^2 + b\mu x$$

has discriminant

$$\Delta_E = 16b^2\mu^2(Z^2 - 4b\mu) = 16b^2\mu^2(c^2 - 4bd)y^2,$$

and hence good reduction outside S^*.

4.4. **A final note.** One last observation which is necessary here 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 3.1, we need also check to see if

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

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

5. Conductors $N = p$ and $N = p^2$

In the case where we want to find elliptic curves E of conductor $N = p$ prime, as noted earlier, things are especially simple. Suppose that E is such curve with invariants c_4 and c_6. From Papadopolous [34], we necessarily have

$$\begin{gathered}(\nu_p(c_4), \nu_p(c_6)) = (0,0) \text{ and } \nu_p(L) \ge 1,\\ (\nu_2(c_4), \nu_2(c_6)) = (0,0) \text{ or } (\ge 4, 3), \text{ and } \nu_2(L) = 6,\\ (\nu_3(c_4), \nu_3(c_6)) = (0,0) \text{ or } (1, \ge 3), \text{ and } \nu_3(L) = 3,\end{gathered}$$

and hence $\mathcal{D} = 1$ or 2. Theorem 3.1 thus implies that there is a cubic form of discriminant ± 4 or $\pm 4p$, and integers u, v, with

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

for some integer n. Similarly, if $N = p^2$, we are interested in finding cubic forms of discriminant $\pm 4 \cdot p^\tau$ for $\tau \in \{0,1,2\}$, and solving $F(x,y) = 8 \cdot p^n$, where $n \in \{0,1\}$ if $\tau = 2$. In this situation, we have that $\mathcal{D} \mid 2p$.

If we first consider the case of a curve E of conductor p, appealing to Théorème 2 of Mestre and Oesterlé [29] (and using [8]), we either have $\Delta_E = \pm p$, or our prime $p \in \{11, 17, 19, 37\}$, or we have $p = t^2 + 64$ for some integer $t \equiv 1 \pmod 4$ and our curve E is isomorphic to that given by

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

Excluding these latter cases, in the notation of the preceding section, we thus have $\alpha_0 = 2$, $\alpha_1 \in \{0,3\}$, $\beta_0 = \beta_1 = 0$, $\kappa_p = 0$ and $N_1 \in \{1,p\}$. We are therefore interested in finding all binary cubic forms (reducible and irreducible) F of discriminant ± 4 and $\pm 4p$ and subsequently solving

$$F(x,y) \in \{1,8\}.$$

Next consider when E has conductor $N = p^2$, so that $p \mid c_4$ and $p \mid c_6$. From (3), we may suppose that $(\nu_p(c_4), \nu_p(c_6), \nu_p(\Delta_E))$ is one of

$$(\geq 1,1,2), (1,\geq 2,3), (\geq 2,2,4), (2,3,\geq 7), (\geq 3,4,8), (3,\geq 5,9) \text{ or } (\geq 4,5,10),$$

or we have that $(\nu_p(c_4), \nu_p(c_6), \nu_p(\Delta_E)) = (\geq 2, \geq 3, 6)$. In this last case, the quadratic twist of our curve E by $(-1)^{(p-1)/2}p$ has good reduction at p and hence conductor 1, a contradiction. If we have $(\nu_p(c_4), \nu_p(c_6), \nu_p(\Delta_E)) = (2,3,\geq 7)$, then E necessarily arises as the $(-1)^{(p-1)/2}p$-twist of a curve of conductor p, say E_1, with corresponding $(\nu_p(c_4(E_1)), \nu_p(c_6(E_1)), \nu_p(\Delta_{E_1})) = (0,0,\nu_p(\Delta_E) - 6)$. Similarly, curves with $(\nu_p(c_4), \nu_p(c_6), \nu_p(\Delta_E)) = (\geq 3,4,8)$ arise as twists of those with $(\nu_p(c_4), \nu_p(c_6), \nu_p(\Delta_E)) = (\geq 1,1,2)$, those with $(\nu_p(c_4), \nu_p(c_6), \nu_p(\Delta_E)) = (3, \geq 5, 9)$ come from ones with $(\nu_p(c_4), \nu_p(c_6), \nu_p(\Delta_E)) = (1, \geq 2, 3)$, and those with $(\nu_p(c_4), \nu_p(c_6), \nu_p(\Delta_E)) = (\geq 4,5,10)$ from ones with $(\nu_p(c_4), \nu_p(c_6), \nu_p(\Delta_E)) = (\geq 2,2,4)$.

Supposing we have already computed all curves of conductor p, it remains therefore, up to twisting, to find $E/\mathbb{Q}$ with minimal discriminant

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

(as noted by Edixhoven, de Groot and Top in Lemma 1 of [20]). In particular, from Theorem 3.1, we are led to consider equations of the shape

$$F(x,y) = 8 \text{ for } F \text{ a form of discriminant } \pm 4p^2, \tag{12}$$

$$F(x,y) = 8p \text{ for } F \text{ a form of discriminant } \pm 4p \tag{13}$$

and

$$F(x,y) = 8p \text{ for } F \text{ a form of discriminant } \pm 4p^2, \tag{14}$$

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

5.1. **Reducible forms.** To find all elliptic curves $E/\mathbb{Q}$ with conductor p or p^2 arising (in the rotation of Theorem 3.1) from reducible forms, we will begin by solving the equation

$$F(x,y) = 8\,p^n, \;\; n \in \mathbb{Z}, \;\; \gcd(x,y) \mid 2,$$

for reducible binary cubic forms of discriminant ± 4, $\pm 4p$ and $\pm 4p^2$. The following result is essentially elementary to prove (if rather painful to state).

Proposition 5.1. *Suppose that $p \geq 3$ is prime and that F is a reducible cubic form with integer coefficients and discriminant $D_F \in \{\pm 4, \pm 4p, \pm 4p^2\}$. If u and v are integers with $\gcd(u,v) \mid 2$, for which we have $F(u,v) = 8p^n$, $n \in \mathbb{Z}$, then, up to $GL_2(\mathbb{Z})$ equivalence, we have one of*

- *$D_F = 4$, $F(u,v) = u^2v + 2uv^2$ and (u,v,p^n) one of*
$$(-17,8,17),(-6,1,3),(-6,2,3),(-4,1,1),(1,8,17),$$
$$(2,-3,3),(2,-2,1),(2,1,1),(2,2,3),(4,-3,3),(4,1,3),$$
- *$D_F = -4$, $F(u,v) = u^2v + 2uv^2 + 2v^3$, with either (u,v,p^n) in*
$$(-23,8,17^2),(-2,2,1),(7,8,17^2),$$
or $n = 1$ and either $p = t^2 + 64$ and $(u,v) = (\pm t - 8, 8)$, or $p = t^2 + 1$ and $(u,v) = (\pm 2t - 2, 2)$, for $t \in \mathbb{N}$.
- *$D_F = -4 \cdot 7$, $F(u,v) = 2u^2v + uv^2 + v^3$ and*
$$(u,v,7^n) \in \{(-4,2,7),(-1,2,1),(-1,4,7),(0,2,1),(3,2,7),(5,1,7)\},$$
- *$D_F = 4 \cdot 3$, $F(u,v) = -u^2v + 2uv^2 + 2v^3$ and $(u,v,3^n) = (-4 \pm 2, -2, 1)$,*
- *$D_F = 4 \cdot 7$, $F(u,v) = -u^2v + 4uv^2 + 3v^3$ and $(u,v,7^n) = (16 \pm 21, 8, 7)$,*
- *$D_F = 4 \cdot 17$, $F(u,v) = 2u^2v + 5uv^2 + v^3$ and $(u,v,17^n) = (1,1,1)$,*
- *$D_F = 4 \cdot 17$, $F(u,v) = -u^2v + 8uv^2 + v^3$ and $(u,v,17^n) = (-32 \pm 33, -8, 1)$,*
- *$D_F = 4 \cdot p$, $F(u,v) = -u^2v + 2[\sqrt{p}]uv^2 + (p - [\sqrt{p}]^2)v^3$ and*
$$(u,v,p^n) = (2[\sqrt{p}], 2, p),$$
Aside : this is equivalent to $F(u,v) = -u^2v + pv^3$ with $(u,v) = (0,2)$.
- *$D_F = 4 \cdot p$ with $p \equiv 1 \pmod 8$,*
$$F(u,v) = -2u^2v + ([\sqrt{p}] - t)uv^2 + (\frac{1}{8}(p - ([\sqrt{p}] - t)^2)v^3,$$
where $t = 1$ if $[\sqrt{p}]$ is even and $t = 0$ if $[\sqrt{p}]$ is odd, and
$$(u,v,p^n) = ([\sqrt{p}] - t, 4, 1),$$
- *$D_F = 4 \cdot p$ with $p = t^2 + 1$, $F(u,v) = -u^2v + 2tuv^2 + v^3$ and*
$$(u,v,p^n) = (2t \pm 2t, 2, 1),$$
- *$D_F = 4 \cdot p$ with $p = t^2 + 8$, $F(u,v) = -u^2v + 2tuv^2 + 8v^3$ and*
$$(u,v,p^n) = (t \pm t, 1, 1),$$
- *$D_F = 4 \cdot p$ with $p = t^2 + 8$, $F(u,v) = -2u^2v + tuv^2 + v^3$ and*
$$(u,v,p^n) = \left(\frac{t \pm t}{2}, 2, 1\right),$$
- *$D_F = 4 \cdot p$ with $p = t^2 - 8$, $F(x,y) = u^2v + 2tuv^2 + 8v^3$ and*
$$(u,v,p^n) = (-t \pm t, 1, 1),$$

- $D_F = 4 \cdot p$ *with* $p = t^2 - 8$, $F(x,y) = 2u^2v + tuv^2 + v^3$ *and*
$$(u, v, p^n) = \left(\frac{-t \pm t}{2}, 2, 1\right),$$
- $D_F = 4 \cdot p$ *with* $p = 16t^2 + 1$, $F(u,v) = 2u^2v + (4t+1)uv^2 + tv^3$ *and*
$$(u, v, p^n) = (4t + 1 \pm 4t, -4, 1),$$
- $D_F = 4 \cdot p$ *with* $p = t^2 + 64$, $F(u,v) = -2u^2v + tuv^2 + 8v^3$ *and*
$$(u, v, p^n) = (0, 1, 1),$$
- $D_F = -4 \cdot 17^2$, $F(u,v) = 17u^2v + 8uv^2 + v^3$ *and*
$$(u, v, 17^n) \in \{(-1, 8, 17), (-32 \pm 15, 136, 17^4)\}.$$
- $D_F = -4 \cdot p^2$ *for* $p \equiv 1 \pmod 4$, $F(u,v) = pu^2v + 2c_0uv^2 + \frac{1}{p}(c_0^2+1)v^3$ *and*
$$(u, v, p^n) = (-2c_0, 2p, p^2), \quad \textit{where } c_0^2 \equiv -1 \pmod p,$$
- $D_F = -4 \cdot p^2$ *with* $p = t^2 + 1$, $F(u,v) = (t^2+1)u^2v + 2tuv^2 + v^3$ *and*
$$(u, v, p^n) \in \{(0, 2, 1), (-2t \pm 2t, 2(t^2+1), p^3)\},$$
- $D_F = -4 \cdot p^2$ *where* $p = t^2 + 64$,
$$F(u,v) = pu^2v + 2c_0uv^2 + \frac{1}{p}(c_0^2+1)v^3 \textit{ where } c_0 \equiv t/8 \pmod p,$$
and
$$(u, v, p^n) \in \{((t - 8c_0)/p, 8, 1), (-8c_0 \pm t, 8p, p^3)\},$$
- $D_F = 4 \cdot 3^2$, $F(u,v) = 3u^2v + 2uv^2$ *and*
$$(u, v, 3^n) \in \left\{\left(-2, \frac{3 \pm 1}{2}, 1\right), \left(2, \frac{-3 \pm 15}{2}, 3^3\right), \left(4, -3 \pm 6, 3^3\right)\right\},$$
- $D_F = 4 \cdot 3^2$, $F(u,v) = 6u^2v + uv^2$ *and*
$$(u, v, 3^n) \in \left\{(-1, 3 \pm 1, 1), \left(1, -3 \pm 15, 3^3\right), \left(2, -6 \pm 12, 3^3\right)\right\},$$
- $D_F = 4 \cdot 17^2$, $F(u,v) = 17u^2v + 2uv^2$ *and*
$$(u, v, 17^n) \in \{(-1, 8, 1), (1, 136, 17^3)\},$$
- $D_F = 4 \cdot 17^2$, $F(u,v) = 34u^2v + uv^2$ *and*
$$(u, v, 17^n) \in \{(8, 17, 17^3), (8, -17^2, 17^3)\},$$
- $D_F = 4 \cdot p^2$, $F(u,v) = pu^2v + 2uv^2$ *and*
$$(u, v, p^n) \in \{(-1 \pm 3, p, p^2), (2, -2p, p^2)\},$$
- $D_F = 4 \cdot p^2$, $F(u,v) = 2pu^2v + uv^2$ *and*
$$(u, v, p^n) \in \left\{\left(\frac{-1 \pm 3}{2}, 2p, p^2\right), (1, -4p, p^2)\right\},$$

To see which elliptic curves can correspond to these reducible forms, it remains to compute

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

where $\mathcal{D} \in \{1, 2, p, 2p\}$. Well-known 2-adic conditions (attributed typically to Kraus or to Connell) and the fact that $\nu_2(\gcd(c_4, c_6)) \leq 3$ imply that either $c_6 \equiv -1 \pmod 4$ or

$$c_4 \equiv 0 \pmod{16} \text{ and } c_6 \equiv 8 \pmod{32}.$$

Under these restrictions, we find the following curves of conductor p or p^2 coming from reducible forms (where, for the sake of concision, we omit quadratic twists by $\pm p$ of conductor p^2). We list a given curve only once – by way of example, the choice of $(b,c,d) = (17,8,1)$ and $(u,v) = (-1,8)$ leads to the same curve one finds by considering $(b,c,d) = (1,2,2)$ and $(u,v) = (7,8)$.

(b,c,d)	(u,v)	(c_4,c_6)	p	Δ_E	N_E
$(1,2,0)$	$(-17,8)$	$(273,4455)$	17	17^2	17
$(1,2,2)$	$(7,8)$	$(33,12015)$	17	-17^4	17
$(1,2,2)$	$(-t-8,8)$	$(p-256,-t(p+512))$	t^2+64	$-p^2$	p
$(2,1,1)$	$(5,1)$	$(105,1323)$	7	-7^3	7^2
$(-1,4,3)$	$(37,8)$	$(1785,75411)$	7	7^3	7^2
$(2,5,1)$	$(1,1)$	$(33,-81)$	17	17^3	17
$(-1,8,1)$	$(1,-8)$	$(4353,287199)$	17	17	17
$(-2,t,8)$	$(0,1)$	$(p-16,-t(p+8))$	t^2+64	p	p

Here, we choose $t \equiv 1 \pmod 4$. We note that the elliptic curves of conductor p or p^2 arising from reducible cubic forms are precisely those with at least one rational 2-torsion point and hence we have another proof of Theorem I of Hadano [23] to the effect that the only such p are $p = 7, 17$ and $p = t^2 + 64$ for integer t.

5.2. **Irreducible forms : conductor p.** It is straightforward to show that there are no irreducible cubic forms of discriminant ± 4. If we begin by searching for elliptic curves of conductor p coming from irreducible cubics, we thus need to solve equations of the shape $F(x,y) = 8$ for all cubic forms of discriminant $\pm 4p$.

5.3. **Irreducible forms : conductor p^2.** As noted earlier, to find the elliptic curves of conductor p^2 coming from irreducible cubics, we need 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).

5.3.1. *Elliptic curves of discriminant $\pm p^3$.* For these, we can use the cubic forms of discriminant $\Delta_F = \pm 4p$ we have already found in the course of computing curves of conductor p, and then solve the Thue equation $F(x,y) = 8p$. We can either do this directly, or reduce this problem to one of solving a pair of new Thue equations of the shape $G_i(x,y) = 8$. To see how this "reduction" proceeds, note, since we assume that $p \,\|\, \Delta_F$, we have, for $F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$,

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

where, since we may suppose that F is a reduced form (whereby $1 \leq a < p$), we necessarily have that $p \nmid a$. We thus obtain

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

$$r_0^2 + 2r_0r_1 \equiv c/a \pmod{p}$$

and

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

From the first two of these, we have

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

and so, assuming that $t^2 \equiv b^2 - 3ac \pmod{p}$,

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

Given these two pairs, we are left to check to see which one satisfies $r_0^2 r_1 \equiv -d/a \pmod{p}$.

To list our pairs (r_0, r_1), we need to find a square root of $b^2 - 3ac$ modulo p. There are efficient ways to do this via the Tonelli-Shanks algorithm, for example (and almost trivially if, say, $p \equiv 3 \pmod{4}$).

Given that we know r_0 and r_1, we thus have, if $F(x, y) = 8p$, either $x \equiv r_0 y \pmod{p}$ or $x \equiv r_1 y \pmod{p}$. In either case, we write $x = r_i y + pu$ so that, from $ax^3 + bx^2y + cxy^2 + dy^3 = 8p$, we are led to solve the two equations $G_i(u, y) = 8$, where

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

We observe 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 $G_i(x, y) = 8$.

We note that there are families of primes for which we can guarantee that the equation $F(x, y) = 8p$ has solutions. For example, if we write $p_{r,s} = r^4 + 9r^2s^2 + 27s^4$, then, if $p = p_{r,s}$ for some choice of integers r and s, we have that the cubic form

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

has discriminant $4p$. Further, we have a polynomial identity $F(x, y) = 8p$ for $x = 2r^2/s + 6s$ and $y = -2r$, or if $x = 6s$ and $y = -18s^2/r - 2r$. In particular, this provides four one-parameter families of primes for which there exists a cubic form F of discriminant $4p$ and integers x and y such that $F(x, y) = 8p$. Specifically, we have, choosing $s \in \{1, 2\}$, in the first case and $r \in \{1, 2\}$ in the second, i.e.

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

Similar, if $p_{r,s} = r^4 - 9r^2s^2 + 27s^4$, the form

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

has discriminant $-4p$. 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 or s in $\{1, 2\}$:

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

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

5.3.2. *Elliptic curves of discriminant p^2 and p^4.* Elliptic curves of discriminant p^2 and p^4 arise from solving the Thue equations $F(x,y) = 8$ and $F(x,y) = 8p$, respectively, for cubic forms F of discriminant $4p^2$. 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

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

From this we are led to solve

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

In the latter case, we may, if we choose, reduce the equation to a single Thue equation of the form $G_{r,s}(x,y) = 8$. To see this, note that we may suppose that $p \nmid y$. It follows that the congruence

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

has a single solution modulo p (since $p^2 \mid \Delta_F$), given (as is readily checked) by $r_0 \equiv 9r^{-1}s \pmod{p}$. We thus have $x \equiv r_0 y \pmod{p}$, so that, writing $x = r_0y + vp$, we have

$$F_{r,s}(r_0y + vp, y) = p(a_0v^3 + b_0v^2y + c_0vy^2 + d_0y^3)$$

and hence, renaming v,

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

where

$$a_0 = sp^2,\ b_0 = (3r_0s+r)p,\ c_0 = 3r_0^2s+2rr_0-9s \text{ and } d_0 = (r_0^3s+rr_0^2-9r_0s-r)/p.$$

We observe that

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

Once again, for our deterministic approach, we solve the equation $F_{r,s}(x,y) = 8p$ directly, while, for our heuristic approach, we consider instead the equation $G_{r,s}(x,y) = 8$.

5.3.3. *Elliptic curves of discriminant $-p^2$ and $-p^4$.* Elliptic curves of discriminant $-p^2$ and $-p^4$ arise from again solving the Thue equations $F(x,y) = 8$ and $F(x,y) = 8p$, respectively, this time for cubic forms F of discriminant $-4p^2$. For such form to exist, we require that $p = |r^2 - 27s^2|$ for integers r and s (so that these primes are precisely those of the form $\pm 1 \pmod{12}$) and find that F is necessarily equivalent to

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

If we wish to solve $F_{r,s}(x,y) = 8p$, as previously, we may note that, if $r_0 \equiv -9r^{-1}s \pmod{p}$, then

$$sr_0^3 + rr_0^2 + 9sr_0 + r \equiv r^{-3}(r^2 - 27s^2)(r^2 + 27s^2) \equiv 0 \pmod{p}.$$

Again write $x = r_0y + vp$, so that, renaming v, we have

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

where now

$$a_0 = sp^2,\ b_0 = (3r_0s+r)p,\ c_0 = 3r_0^2s+2rr_0+9s \text{ and } d_0 = (r_0^3s+rr_0^2+9r_0s+r)/p.$$

While it is not immediately obvious that, given we know the existence of integers r and s such that $p = |r^2 - 27s^2|$, we can actually find them, it is, in fact, computationally straightforward to do so, via the following result :

Proposition 5.2. *If $p \equiv 1 \pmod{12}$ is prime, there exist positive integers r and s such that*

$$r^2 - 27s^2 = p$$

and

$$r < \frac{3}{2}\sqrt{6p}, \quad s < \frac{5}{18}\sqrt{6p}.$$

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

$$r^2 - 27s^2 = -p$$

and

$$r < \frac{5}{2}\sqrt{2p}, \quad s < \frac{1}{2}\sqrt{2p}.$$

As a final comment, we note that if 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

$$s_1x^3 + r_1x^2y + 9s_1xy^2 + r_1y^3 \quad \text{and} \quad s_2x^3 + r_2x^2y + 9s_2xy^2 + r_2y^3$$

are readily seen to be $\mathrm{GL}_2(\mathbb{Z})$-equivalent.

6. Computational details

The computations required to generate curves of prime conductor p (and subsequently conductor p^2) fall into a small number of distinct parts.

6.1. **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 4, we generated all reduced forms $F(x, y) = ax^3 + bx^2y + cxy^2 + d$ with discriminants in $(0, 4X]$ and $[-4X, 0)$, separately, by looping over a finite set of a, b, c, d values as prescribed by Lemmata 4.2 and 4.4, respectively. 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 [30], [37]; to make this deterministic for the range we require, we appeal to [40]). While it is straightforward to code the above in computer algebra packages such as `sage`, `maple` or `magma`, we instead implemented it in `c++` for speed. To avoid possible numerical overflows, we used the `CLN` library [24] for `c++`.

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 parallelised 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 than ran $a = 1, 2$ with the master node distributing b-values to the other cores. The total CPU time was about 3 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.

We then sorted the forms into discriminant order, while keeping positive and negative discriminant separated. Sorting a terabyte of data is a non-trivial 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 forms took around 2 days of real time.

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

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

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 [44], 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` and Pari/GP. 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`, 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 into corresponding elliptic curves in minimal form using Theorem 3.1 and standard techniques.

For positive discriminant, this approach works without issue for $p < 10^{10}$. For negative discriminant, however, the fundamental units in the associated cubic field can be extremely large (in the neighbourhood of $e^{\sqrt{p}}$). For this reason, finding all negative discriminant curves with prime conductor exceeding $2 \cdot 10^9$ or so proves to be extremely slow. Consequently, for large p, we turned to a non-exhaustive method, which, though it finds solutions to the Thue equation, is not actually guaranteed to find them all.

6.3. **Non-exhaustive, 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 quick computational 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

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

either have that x and y are small, 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 an approach was developed in detail by Attila Pethő [35], [36]; 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 $n\in[0,999]$.

6.4. **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 3.1 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,a_6 for a corresponding elliptic curve in minimal form (see e.g. Cremona [14]). 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.

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

6.5.1. *Twisting conductor p.* The vast majority of forms of conductor p^2 are quadratic twists of curves of conductor p. To compute these we took all curves with conductor $p\leq 10^{10}$ and computed c_4 and c_6. The twisted curve then has corresponding c-invariants

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

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.

6.5.2. *Solving $F(x,y)=8p$ with F of discriminant $\pm 4p$.* There was no need to find 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 non-exhaustive, heuristic method, we first converted the equation to a pair of new Thue equations of the form $G_i(x,y) = 8$ as described in Section 5.3.1 and then applied Pethő's solution search method.

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 search for more curves of conductor p^2.

6.5.3. *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 5.3.2, 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 non-exhaustive 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 5.3.2. The process for forms of discriminant $-4p^2$ was very similar, excepting that more care is required with the range of r and s. The non-exhaustive 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 search for other curves of conductor p^2.

7. Data

7.1. **Previous work.** The principal prior work on computing table of elliptic curves of prime conductor was carried out in two lengthy computations, by Brumer and McGuinness [9] in the late 1980s and by Stein and Watkins [42] 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).

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

X	$\Delta_E > 0$	$\Delta_E < 0$	Ratio^2	Total	Expected
10^3	33	52	2.4830	85	68
10^4	130	228	3.0760	358	321
10^5	625	1116	3.1884	1741	1669
10^6	3388	5913	3.0460	9301	9223
10^7	19606	34006	3.0084	53612	52916
10^8	114453	198041	2.9940	312494	311587
10^9	685278	1187687	3.0038	1872965	1869757
10^{10}	4171055	7226983	3.0021	11398038	11383665
10^{11}	25661634	44466340	3.0026	70127974	70107401
10^{12}	159552514	276341397	2.9997	435893911	435810488

The data above the line is rigorous (in case of positive discriminant); for negative discriminant, we have a rigorous result only up to 2×10^9. For the positive forms this took about 1 week of real time using 80 cores. Unfortunately, the negative discriminant forms took significantly longer, roughly 2 months of real times using 80 cores. Heuristics given by Brumer and McGuinness [9] 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 $N_E \leq X$ 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 $-p^2$.

7.3. **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 $-4p$, curves from discriminant $+4p^2$ and $-4p^2$. The list was then sorted and any duplicates removed. The resulting list is approximately 1 gigabyte. The counts of curves are below.

X	$\Delta_E > 0$	$\Delta_E < 0$	Total	Ratio^2
10^3	53	94	147	3.1456
10^4	192	322	514	2.8126
10^5	765	1304	2069	2.9056
10^6	3764	6357	10121	2.8524
10^7	20540	35096	55636	2.9195
10^8	116895	200799	317694	2.9507
10^9	691806	1195263	1887069	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 1 day on a single core.

The only curves of real 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 found by Edixhoven, de Groot and Top [20] (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 $p \leq X$:

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 5.3.2 and 5.3.3, 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 5.3.1.

7.4. **Thue equations.** It is worth noting that all solutions we encountered to the Thue equations $F(x, y) = 8$ and $F(x, y) = 8p$ we treated were with $|x|, |y| < 2^{30}$. The "largest" such solution corresponded to the equation

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

with solution

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

This leads to the elliptic curve of conductor 948762329069,

$$y^2 + xy + y = x^2 - 2x^2 + a_4x + a_6,$$

with

$$a_4 = -1197791024934480813341$$

and

$$a_6 = 1595584083717556524357956436864 1.$$

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	24	23	79	62
10^4	205	163	741	453
10^5	1852	1159	6105	2641
10^6	16334	7668	53203	16079
10^7	147654	49867	466602	97074
10^8	1330935	314722	4126542	582792
10^9	12050911	1966105	36979558	3530820
10^{10}	109730654	12229663	334260482	21576585
10^{11}	1004607004	76122366	3045402452	133115651
10^{12}	9247369050	475831852	27938060315	828238359

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).

7.5. **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 believes new heuristics that predict that the Mordell-Weil rank of $E/\mathbb{Q}$ is absolutely bounded, then this number should also be so bounded. As noted by Brumer and Silverman [10], 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 :

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

Of these 20 curves, 2 have rank 3, 3 have rank 2, 9 have rank 1 and 6 have rank 0. All have discriminant $-p$. The class group of $\mathbb{Q}(\sqrt{3 \cdot 530956036043})$ is isomorphic to

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z},$$

which, via a classical result of Hasse [25], explains the existence of a large number of cubic forms of discriminant $-4p$. Elkies [21] found examples of rather larger conductor with more curves, including 21 for $p = 14425386253757$ and discriminant p, 24 for $p = 998820191314747$ and discriminant $-p$.

7.6. **Rank and discriminant records.** In the following table, we list the smallest prime conductor with a given Mordell-Weil rank.

N	$[a_1, a_2, a_3, a_4, a_6]$	$\mathrm{sign}(\Delta_E)$	$rk(E(\mathbb{Q}))$
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 [22]).

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

N	$[a_1, a_2, a_3, a_4, a_6]$	$\mathrm{sign}(\Delta_E)$	$rk(E(\mathbb{Q}))$
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

7.7. **Completeness.** We will conclude with a few remarks on how likely it is that we have missed any curves of conductor $p < 10^{12}$ (other than potentially through data corruption or something similar). A conjecture of Hall, widely disbelieved without modification at present, admittedly, is that if x and y are integers for which $x^3 - y^2$ is nonzero, then the *Hall ratio*

$$\frac{|x|^{1/2}}{|x^3 - y^2|}$$

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

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

discovered by Elkies, with $\frac{|x|^{1/2}}{|x^3-y^2|} > 46.6$. If there is an elliptic curve we have missed with conductor $p < 10^{12}$, then, from the identity $|c_4^3 - c_6^2| = 1728p$, we have a Hall ratio

$$\frac{|c_4|^{1/2}}{1728p} > \frac{|c_4|^{1/2}}{1.728 \cdot 10^{15}}. \tag{15}$$

Since we have $c_4 = \mathcal{D}^2 H_F(u, v)$ for $\mathcal{D} \in \{1, 2\}$, and since we have checked all possible solutions with $\min\{|u|, |v|\} \leq 10^{30}$ or so, we may assume that $\min\{|u|, |v|\} > 10^{30}$, whereby it is possible to show that $|c_4| > 10^{59}$ (more generally, if we assume that $\min\{|u|, |v|\} > X$, we have that $|c_4| \gg X^2$). It follows that any elliptic curve of prime conductor $p < 10^{12}$ that we have missed necessarily leads to a Hall ratio in excess of 10^{14}.

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), 991–1002.

[2] K. Belabas. *A fast algorithm to compute cubic fields,* Math. Comp. 66 (1997), 1213–1237.

[3] K. Belabas and H. Cohen, *Binary cubic forms and cubic number fields*, Organic Mathematics (Burnaby, BC, 1995), 175–204. CMS Conf. Proc., 20 Amer. Math. Soc. 1997.

[4] M. A Bennett and A. Ghadermarzi, *Mordell's equation : a classical approach*, L.M.S. J. Comput. Math. 18 (2015), 633–646.

[5] M. A. Bennett and A. Rechnitzer, *Computing elliptic curves over* $\mathbb{Q}$, submitted for publication.

[6] W. E. H. Berwick and G. B. Mathews, *On the reduction of arithmetical binary cubic forms which have a negative determinant*, Proc. London Math. Soc. (2) 10 (1911), 43–53.

[7] B. J. Birch and W. Kuyk (Eds.), *Modular Functions of One Variable IV*, Lecture Notes in Math., vol. 476, Springer-Verlag, Berlin and New York, 1975.

[8] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the Modularity of Elliptic Curves over* $\mathbb{Q}$ *: Wild 3-adic Exercises*, J. Amer. Math. Soc. 14 (2001), 843–939.

[9] A. Brumer and O. McGuinness, *The behaviour of the Mordell-Weil group of elliptic curves*, Bull. Amer. Math. Soc. 23 (1990), 375–382.

[10] A. Brumer and J. H. Silverman, *The number of elliptic curves over* $\mathbb{Q}$ *with conductor* N, Manuscripta Math. 91 (1996), 95–102.

[11] 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.

[12] F. Coghlan, *Elliptic Curves with Conductor* 2^m3^n, Ph.D. thesis, Manchester, England, 1967.

[13] J. Cremona, *Elliptic curve tables*, `http://johncremona.github.io/ecdata/`

[14] J. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997. Available online at `http://homepages.warwick.ac.uk/staff/J.E.Cremona/book/fulltext/index.html`

[15] J. Cremona, *Reduction of binary cubic and quartic forms,* LMS J. Comput. Math. 4 (1999), 64–94.

[16] J. Cremona and M. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Experiment. Math. 16 (2007), 303–312.

[17] H. Davenport, *The reduction of a binary cubic form. I.*, J. London Math. Soc. 20 (1945), 14–22.

[18] H. Davenport, *The reduction of a binary cubic form. II.*, J. London Math. Soc. 20 (1945), 139–147.

[19] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II.*, Proc. Roy. Soc. London Ser. A. 322 (1971), 405–420.

[20] B. Edixhoven, A. de Groot and J. Top, *Elliptic curves over the rationals with bad reduction at only one prime*, Math. Comp. 54 (1990), 413–419.

[21] N. D. Elkies, *How many elliptic curves can have the same prime conductor?*, `http://math.harvard.edu/~elkies/condp_banff.pdf`

[22] N. D. Elkies, and M. Watkins, *Elliptic curves of large rank and small conductor*, Algorithmic number theory, 42–56, Lecture Notes in Comput. Sci., 3076, Springer, Berlin, 2004.

[23] T. Hadano, *On the conductor of an elliptic curve with a rational point of order* 2, Nagoya Math. J. 53 (1974), 199–210.

[24] B. Haible, *CLN, a class library for numbers*, available from `http://www.ginac.de/CLN/`

[25] H. Hasse, *Arithmetische Theorie der kubischen Zahlköper auf klassenkörpertheoretischer Grundlage*, Math. Z. 31 (1930), 565–582.

[26] C. Hermite, *Note sur la réduction des formes homogènes à coefficients entiers et à deux indéterminеées*, J. reine Angew. Math. 36 (1848), 357–364.

[27] C. Hermite, *Sur la réduction des formes cubiques à deux indéxterminеées*, C. R. Acad. Sci. Paris 48 (1859), 351–357.

[28] G. Julia, *Étude sur les formes binaires non quadratiques à indéterminés rélles ou complexes*, Mem. Acad. Sci. l'Inst. France 55 (1917), 1–293.

[29] J.-F. Mestre and J. Oesterlé. *Courbes de Weil semi-stables de discriminant une puissancemième*, J. reine angew. Math 400 (1989), 173–184.

[30] G. L. Miller, *Riemann's hypothesis and tests for primality* in Proceedings of seventh annual ACM symposium on Theory of computing, 234–239 (1975).
[31] L. J. Mordell, *The diophantine equation* $y^2 - k = x^3$, Proc. London. Math. Soc. (2) 13 (1913), 60–80.
[32] L. J. Mordell, *Diophantine Equations,* Academic Press, London, 1969.
[33] O. Neumann, *Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten II*, Math. Nach. 56 (1973), 269–280.
[34] I. Papadopolous, *Sur la classification de Néron des courbes elliptiques en caract´ristique résseul* 2 *et* 3, J. Number Th. 44 (1993), 119–152.
[35] A. Pethő, *On the resolution of Thue inequalities*, J. Symbolic Computation 4 (1987), 103–109.
[36] A. Pethő, *On the representation of* 1 *by binary cubic forms of positive discriminant*, Number Theory, Ulm 1987 (Springer LNM 1380), 185–196.
[37] M. O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Th. 12 (1980) 128–138.
[38] B. Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. 10 (1975), 367–378.
[39] I. R. Shafarevich, *Algebraic number theory*, Proc. Internat. Congr. Mathematicians, Stockholm, Inst. Mittag-Leffler, Djursholm (1962), 163–176.
[40] J. P. Sorenson and J. Webster, *Strong Pseudoprimes to Twelve Prime Bases*, arXiv preprint arXiv:1509.00864.
[41] V. G. Sprindzuk, *Classical Diophantine Equations*, Springer-Verlag, Berlin, 1993.
[42] W. Stein and M. Watkins, *A database of elliptic curve – first report*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Compute. Sci., vol. 2369, Springer, Berlin, 2002, pp. 267–275.
[43] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. Reine Angew Math. 135 (1909), 284–305.
[44] N. Tzanakis and B. M. M. de Weger, *On the practical solutions of the Thue equation*, J. Number Theory 31 (1989), 99–132.
[45] N. Tzanakis and B. M. M. de Weger, *Solving a specific Thue-Mahler equation*, Math. Comp. 57 (1991) 799–815.
[46] N. Tzanakis and B. M. M. de Weger, *How to explicitly solve a Thue-Mahler equation*, Compositio Math., 84 (1992), 223–288.
[47] M. Watkins, *Some heuristics about elliptic curves*, Experiment. Math. 17 (2008), 105–125.
[48] B. M. M. de Weger, *Algorithms for diophantine equations*, CWI-Tract No. 65, Centre for Mathematics and Computer Science, Amsterdam, 1989.
[49] B. M. M. de Weger, *The weighted sum of two S-units being a square*, Indag. Mathem. 1 (1990), 243–262.

Department of Mathematics, University of British Columbia, Vancouver BC
E-mail address: bennett@math.ubc.edu

Department of Mathematics, University of British Columbia, Vancouver BC
E-mail address: andrewr@math.ubc.edu