

# ON ELLIPTIC CURVES OF CONDUCTOR $N=PQ$

SEAN HOWE (DRAFT OF 3 MAY 2010)

ABSTRACT. We study elliptic curves with conductor  $N = pq$  for  $p$  and  $q$  prime. By studying the 2-torsion field we obtain that for  $N$  a product of primes satisfying some congruency conditions and class number conditions on related quadratic fields, any elliptic curve of conductor  $N$  has a rational point of order 2. By studying a minimal Weierstrass equation and its discriminant we obtain a solution to some Diophantine equation from any curve with conductor  $N = pq$  and a rational point of order 2. Under certain congruency conditions, this equation has no solutions, and so we conclude that in this situation there is no elliptic curve of conductor  $N$  with a rational point of order 2. Combining these two results, we prove that for a family of  $N = pq$  satisfying more specific congruency conditions and class number conditions on related quadratic fields, there are no elliptic curves of conductor  $N$ . We use a computer to find all  $N < 10^7$  satisfying these conditions, of which there are 67. This work is similar to and largely inspired by past work on conductors  $p$  by Ogg [14, 15], Hadano [9], Neumann [13], Setzer [17], and Brumer and Kramer [4].

## CONTENTS

1. Introduction	1
2. Elliptic Curves and Conductors	3
3. Prior Work	4
3.1. Conductors of the form $2^m 3^n$	4
3.2. Prime power conductors	5
3.3. Conductors of the form $2^m p$	6
4. Curves with no rational point of order 2	6
4.1. Examining the 2-torsion field	7
4.2. Forcing a rational point of order 2	8
5. Curves with a rational point of order 2	9
5.1. Diophantine Setup	9
5.2. Diophantine Solutions	11
5.3. Non-existence of curves with a rational point of order 2	12
6. Non-existence of elliptic curves with certain conductors $pq$	13
7. Future work	14
8. Source code	15
References	16

## 1. INTRODUCTION

In 1999, after six years of careful labor following the first announcement of Wiles' breakthrough work, a full proof of the famous Taniyama-Shimura-Weil conjecture

was completed. The conjecture provides a correspondence between elliptic curves and modular forms with far-reaching implications – for instance, the partial results of the original paper by Wiles [20] were sufficient to give a proof of Fermat’s Last Theorem. The conjecture is now known as the Modularity Theorem, and we give an approximate statement below:

**Theorem** (Modularity Theorem). *Let  $E/\mathbb{Q}$  be an elliptic curve. Then there exists a rational map  $X_0(N) \rightarrow E$  where  $X_0(N)$  is the classical modular curve and  $N$  is the conductor of  $E$ .*

Darmon [7] provides a more detailed description of the work leading up to the full proof as well as an accessible account of the correspondence between weight 2 newforms and elliptic curves implied by the Modularity Theorem. He also offers further discussion of the proof’s importance in mathematics.

In this work, we will be concerned primarily with the conductors of elliptic curves, which figure prominently in the statement of the Modularity Theorem. Indeed, much of the research on the conductors of elliptic curves done between the late 1960s and the early 1990s was done with an eye toward providing evidence for the validity of the Taniyama-Shimura-Weil conjecture. The idea was to classify all the curves of some specific conductors  $N$  and then compare that data against the corresponding data about modular forms - if it did not match up, the conjecture would be disproven, and if it did match up, then there would be more reason to think the conjecture true. In particular, a large amount of work was put in to proving that there were no elliptic curves of certain prime conductors for which it was already known that there were no weight 2 newforms. In Section 3 we will discuss some of these results and the techniques used to achieve them.

Many of the results that were proved in order to provide support for the Modularity Theorem were superseded by its proof. Indeed, even before Wiles’ 1993 announcement, Cremona [6] had already provided effective algorithms to calculate all isogeny classes of modular elliptic curves of a given conductor, and the Modularity Theorem implies that all elliptic curves are modular and so these algorithms in fact calculate all isogeny classes of elliptic curves of a given conductor. These algorithms have been run for all conductors  $N < 130000$  and tables of the results are available online through John Cremona’s website [5].

However, the study of conductors of elliptic curves has importance beyond just the verification of the modularity theorem, and there are a variety of questions about conductors that remain unanswered despite the effective algorithms provided by the Modularity Theorem. In particular, although the Modularity Theorem provides an effective method of classifying all elliptic curves of a specific conductor, it does not allow us to make a statement about the existence or non-existence of elliptic curves for interesting infinite families of conductors. The goal of this thesis was to try to expand upon some of the methods used to provide early evidence for the Modularity Theorem in order to be able to prove such an infinite statement, paying particular attention to the family of conductors  $N = pq$  for distinct primes  $p$  and  $q$ . In the end we were not able to provide such a statement. However, by using methods similar to those pioneered by Ogg [14, 15], Hadano [9], Neumann [13], and Setzer [17], we were able to prove a non-existence result (Theorem 6.1) for a family of  $N = pq$  where  $p$  and  $q$  satisfy certain congruency conditions and some related quadratic fields satisfy certain class number conditions. This family could be infinite, and indeed by Dirichlet’s theorem the congruency conditions pose no

obstacle to this, but it is unknown whether or not the class number conditions are satisfied in infinitely many cases. By running a computer search, we found 67 values of  $N < 10^7$  satisfying these conditions. These are listed in a table at the end of Section 6. Of these 67, only one was less than 130000 and therefore 66 of them are not contained in Cremona's Tables. For these 66 values of  $N$ , this non-existence is a new result.

Before we begin, I'd like to thank Professor Kirti Joshi of the University of Arizona math department for advising me on this thesis.

## 2. ELLIPTIC CURVES AND CONDUCTORS

An *elliptic curve* is a smooth, projective algebraic curve of genus one together with a distinguished point lying on the curve that we use to define a group law. Any elliptic curve  $E$  can be given as the zero set of a cubic equation with the distinguished point lying at infinity and if it's possible to find such an equation with coefficients in the field  $K$  then we say that  $E$  is an elliptic curve defined over  $K$  and write  $E/K$ . Viewing curves as the zeros of cubic equations, two equations give the same curve if there is a  $K$ -rational change of coordinates taking one to the other and fixing the point at infinity. The form of an equation for such a curve is called Weierstrass form and if  $K$  is a field of characteristic not equal to 2 or 3 then any elliptic curve over  $K$  can be given by a simplified Weierstrass equation of the form

$$(2.1) \quad E : y^2 = x^3 + ax + b$$

with  $a, b \in K$  and the discriminant  $4a^3 + 27b^2 \neq 0$  [18].

If  $E/K$  is an elliptic curve then the points on  $E$  with coordinates contained in an extension  $L/K$  form a group under the group law and we will denote this subgroup by  $E(L)$  [18, ch. 3]. A question of fundamental importance in the study of elliptic curves is, for an elliptic curve defined over a number field  $K$ , what is the group structure of  $E(K)$ ? A seminal result, the Mordell-Weil theorem, states that this group is finitely generated [18, ch. 8]. For elliptic curves over  $\mathbb{Q}$ , work by Lutz, Nagell, and more recently Mazur, has firmly established the structure of the torsion subgroup of  $E(\mathbb{Q})$ . The question of the rank of  $E(\mathbb{Q})$ , however, remains relatively wide open, and more generally the question of the rank of  $E(K)$  for any number field  $K$ . The latter is the subject of the Birch and Swinnerton Dyer conjecture, a Millenium Prize problem and one of the most important unsolved problems in number theory, which relates the rank of an elliptic curve to the order of the zero of its associated  $L$ -function at  $s = 1$ .

Elliptic curves also find significant use in applied mathematics. They are used heavily in cryptography due to the presumed difficulty of the discrete log problem on an elliptic curve over a finite field, and in a related vein they are also used in factoring algorithms and primality tests.

A common technique in the study of elliptic curves over  $\mathbb{Q}$  is to consider them as curves over the  $p$ -adic numbers - if  $E/\mathbb{Q}$  is an elliptic curve then we can consider the group  $E(\mathbb{Q}_p)$ . A natural map that arises in this context is the reduction mod  $p$  map: after a change of coordinates we can write an equation for  $E$  in Weierstrass form as in (2.1) with  $a, b$  integers, and after taking a "minimal" such equation, we can reduce the coefficients mod  $p$  to obtain a curve  $\tilde{E}/\mathbb{F}_p$  (indeed, by considering a more general form of the elliptic curve equation we can find an equation that

is minimal at all primes). Note that any point on  $E(\mathbb{Q}_p)$  can be written uniquely as  $[x : y : z]$  with each of  $x$ ,  $y$ , and  $z$  contained in  $\mathbb{Z}_p$  and at least one in the units group  $\mathbb{Z}_p^\times$ , and so reduction of the coordinates mod  $p$  makes sense and in fact provides a homomorphism from  $E(\mathbb{Q}_p)$  to  $\tilde{E}(\mathbb{F}_p)$ . This restricts to a very useful homomorphism  $E(\mathbb{Q}) \rightarrow \tilde{E}(\mathbb{F}_p)$  - for instance, we can use it to determine the structure of the torsion subgroup as it can be shown that if we restrict to the  $m$ -torsion in  $E(\mathbb{Q})$  then this reduction mod  $p$  map becomes an injection (note that this is contingent upon  $\tilde{E}$  being nonsingular) [18, ch. 7].

An interesting question to ask is what happens when  $\tilde{E}$  is a singular curve? This phenomenon is called *bad reduction*, and can occur in two ways: if  $\tilde{E}$  has a cuspidal singularity then we call it additive reduction and if it has a nodal singularity we call it multiplicative reduction (the names coming from the fact that singular curves are isomorphic to either the additive or multiplicative subgroups of the base field). An elliptic curve can only have bad reduction at finitely many primes, namely those that divide its discriminant (though it is not necessarily true that an elliptic curve given by a Weierstrass equation has bad reduction at every prime dividing its discriminant - it may be possible to make a rational change of variables to obtain a new Weierstrass equation whose discriminant is not divisible by that prime) [18, ch. 7]. For an elliptic curve  $E/\mathbb{Q}$  (or more generally any number field with class number 1), there is always a Weierstrass form whose discriminant is minimal in the sense that it divides the discriminant of all other Weierstrass forms for  $E$ .

To understand the group structure of  $E(\mathbb{Q})$  it is important to understand at which primes it has bad reduction - for instance, the terms used in defining the curve's  $L$ -function, which as mentioned earlier is connected to the rank of  $E(\mathbb{Q})$ , differ between primes where bad reduction occurs and primes where it does not.

The information about the reduction of an elliptic curve is encoded in an invariant called the conductor. The conductor has an intrinsic definition in terms of the Néron model [18, Appx. C], but for our purposes we can view the conductor in a simpler manner: For an elliptic curve  $E/\mathbb{Q}$ , the conductor  $N$  is a positive integer divisible only by the primes where  $E$  has bad reduction. Furthermore, if  $E$  has multiplicative reduction at  $p$  then  $p$  divides  $N$  exactly once, and if  $E$  has additive reduction at  $p$  then  $p^2|N$  and for  $p \geq 5$  if the curve has additive reduction at  $p$  then  $p$  divides  $N$  exactly twice [8].

### 3. PRIOR WORK

In this section we will make a brief summary of prior work, noting where it has been superseded by the Modularity Theorem and Cremona's algorithm.

**3.1. Conductors of the form  $2^m 3^n$ .** Elliptic curves with these conductors were completely classified before the Modularity Theorem was proven. The most elementary result, that there is no elliptic curve over  $\mathbb{Q}$  of conductor 1, can be found in Ogg [14] where the Diophantine argument given is attributed to Tate. Ogg also provided the first results for two-power conductors in [14], and in his following paper [15] he classified curves with conductor  $3 \cdot 2^n$  and  $9 \cdot 2^n$ . Ogg used a powerful technique whereby he combined the careful study of the 2-division field and Diophantine analysis; this technique is used in most of the following work. The full classification is widely attributed to Coghlan in his PhD Thesis, but I cannot

find enough information to provide a full reference. Hadano [9] has an alternative approach to conductors of the form  $3^n$ , and a complete classification of these curves can be found in [2, pp. 123-134]. The Modularity Theorem and Cremona's algorithm provide alternate proofs for all of these results.

**3.2. Prime power conductors.** Setzer [17] proved the following existence/non-existence result:

**Theorem 3.1** (Setzer [17]). *Let  $p$  be a prime s.t.  $p \neq 2, 3, 17$ . There is an elliptic curve of conductor  $p$  over  $\mathbb{Q}$  with a rational point of order 2 if and only if  $p = u^2 + 64$  for some rational integer  $u$ . If  $p$  is of the form  $u^2 + 64$ , there are, up to isomorphism, just two such curves.*

Slightly weaker but similar forms of this theorem were proven by Hadano [9] and Neumann [13]. It is unknown whether or not there are infinitely many primes of the form  $u^2 + 64$ , so we cannot say whether or not this is supplanted by the Modularity Theorem. We see here that the hypothesis includes the existence of a rational torsion point, and in general this greatly simplifies the Diophantine analysis needed. Indeed, Miyawaki [11] was able to classify all curves of prime power conductor with at least three rational torsion points. A standard strategy, again stretching back to Ogg, for showing that no elliptic curves of a certain conductor exists, is to show that any such elliptic curve must have a rational two-torsion point and then show that any such elliptic curve with a rational two-torsion point would give rise to a solution of an insoluble Diophantine equation. This, for instance, is how he proves the following theorem:

**Theorem 3.2** (Ogg [15]). *An abelian curve of conductor  $10, 14, 22, 30, 34, 90$  has a rational point of order 2 and there are no elliptic curves of conductor 10 or 22.*

Of course, results like this that only apply to a finite lists of conductors are completely superseded by the Modularity Theorem and Cremona's algorithm. However, similar results such as the following, which cover a possibly infinite set of conductors, remain interesting:

**Theorem 3.3** (Setzer [17]). *Let  $p$  be a prime such that  $p \equiv \pm 1 \pmod{8}$ . If the class numbers of both  $\mathbb{Q}(\sqrt{p})$  and  $\mathbb{Q}(\sqrt{-p})$  are not divisible by 3, then each elliptic curve of conductor  $p$  defined over  $\mathbb{Q}$  has a rational point of order 2.*

Setzer combined Theorems 3.1 and 3.3 in order to prove non-existence of curves of certain prime conductors, another example of Ogg's strategy. Brumer and Kramer [4] also further expanded upon the techniques of Ogg, using the work of Serre [16] to improve the analysis of the 2-torsion field and also analyze the 3-torsion field. Their extension of these techniques remains interesting, although the specific non-existence results they obtained with them are superseded by the Modularity Theorem. Indeed, their results directly imply our Theorem 4.8, although the proof we present in this paper is more elementary in that it uses only the basic class field theory techniques of Ogg and Setzer.

There is another interesting extension of these techniques by Boston:

**Theorem 3.4** (Boston [3]). *Let  $N$  be a prime  $\equiv 3 \pmod{8}$  such that 3 does not divide the class numbers of  $\mathbb{Q}(\sqrt{\pm N})$ . Let  $M$  be one of the cubic subfields of the unique cubic extension of  $\mathbb{Q}(\sqrt{-N})$  of conductor (2). Suppose that  $h(M)$  is odd and that the minimal polynomial modulo  $N$  of  $M$  has a quadratic residue and a quadratic*

non-residue root. Then there is at most one isogeny class of elliptic curve over  $\mathbb{Q}$  of conductor  $N$  with given trace of Frobenius at  $2$ ,  $a_2$ .

Agrawal, *et al.* [1] provides a classification of the curves of conductor 11, the first really difficult non-trivial case, but this is obviously superseded by the Modularity Theorem. Edixhoven, *et al.* [8] provide some results on curves of conductor  $p^2$ , proving most notably the following:

**Theorem 3.5** (Edixhoven, *et. al* [8]). *If  $p$  is a prime number and  $p \equiv 5 \pmod{12}$ , then every elliptic curve over  $\mathbb{Q}$  with conductor  $p^2$  is a twist of one of conductor  $p$ .*

This theorem, combined with earlier non-existence results on curves of conductor  $p$ , allowed them to prove the non-existence of curves of conductor  $p^2$  for many primes. These results have been superseded by the Modularity Theorem, but the theorem itself remains interesting, especially if it could be combined with a general non-existence result on curves of conductor  $p$ .

**3.3. Conductors of the form  $2^m p$ .** Hadano provides the following non-existence results:

**Theorem 3.6** (Hadano [9]). *If none of the class numbers of the four quadratic fields  $\mathbb{Q}(\sqrt{\pm p})$  and  $\mathbb{Q}(\pm 2p)$  for a prime  $p \equiv 3$  or  $5 \pmod{8}$  are divisible by 3, then there are no elliptic curves of conductor  $N = 2p$ .*

**Theorem 3.7** (Hadano [9]). *If none of the class numbers of the four quadratic fields  $\mathbb{Q}(\sqrt{\pm p})$  and  $\mathbb{Q}(\pm 2p)$  for a prime  $p \equiv 1$  or  $7 \pmod{8}$  are divisible by 3, then an elliptic curve of conductor  $N = 2^m p$  ( $m > 0$ ) has a rational point of order 2.*

In addition, he gives the following classification result:

**Theorem 3.8** (Hadano [9]). *For any  $p \equiv 3$  or  $5 \pmod{8}$  satisfying the conjecture of Ankeny-Artin-Chowla (or its analogy for  $p \equiv 3 \pmod{4}$ ), all elliptic curves of conductor  $N = 2^m p^n$  can be effectively determined. If  $p - 2$  or  $p - 4$  is a square number, then the assumption that the conjecture holds can be dropped.*

By effectively determined, he means that the problem can be reduced to checking for the existence of solutions to finitely many Diophantine equations. The conjecture of Ankeny-Artin-Chowla and its analogy for  $p \equiv 3 \pmod{4}$  can be found in Mordell's book on Diophantine equations [12, Ch. 8]. This theorem is in some sense superseded by the Modularity Theorem and Cremona's algorithms, as they also provide a method for classifying all such curves.

#### 4. CURVES WITH NO RATIONAL POINT OF ORDER 2

The goal of this section is to prove Theorem 4.8. We will do so using the methods of Ogg [14, 15] and Setzer [17], thereby providing a proof of the theorem that uses only basic class field theory. It should be noted though that this result also follows directly from the work of Brumer and Kramer [4, Cor. 5.3], who use the machinery developed by Serre in [16], and in some sense theirs is a more modern approach.

In 4.1 we fix some terminology and develop some basic facts about the 2-torsion fields of elliptic curves with no rational point of order 2. Our Lemmas 4.1 through 4.5 are lifted directly from Ogg [14, 15] (though they are not all listed as lemmas there), but we restate and reprove them here for clarity, sometimes also providing alternate proofs and/or elaborating on the original proofs. In 4.2 we use these

results to build toward Theorem 4.8 which provides conditions on a product of primes  $N = p_1 \dots p_n$  that force any elliptic curve with conductor  $N$  to have a rational point of order 2.

**4.1. Examining the 2-torsion field.** In the sequel let  $E/\mathbb{Q}$  be an elliptic curve with no rational point of order 2 and let  $k = \mathbb{Q}(\sqrt{\Delta})$  for  $\Delta$  the discriminant of any Weierstrass form for  $E$ . (Note that the discriminants of different Weierstrass forms differ by powers of 12 so this field is well-defined). Let  $K = \mathbb{Q}(E[2])$  where  $E[2]$  is the 2-torsion of  $E$  (again note this field is well defined as a rational change of coordinates sends points of order 2 to points of order 2), and note  $K$  is Galois over  $\mathbb{Q}$ . If we take a Weierstrass equation for  $E$ :

$$(4.1) \quad E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 = f(x)$$

then  $16\Delta = d$  where  $d$  is the discriminant of  $f$ , so  $k = \mathbb{Q}(\sqrt{d})$ . Now,  $f(x)$  is irreducible over  $\mathbb{Q}$  since any root would give a rational point of order 2, and so, by standard algebraic result,  $K$ , which is obtained by adjoining all of the roots of  $f$ , is a degree 3 cyclic extension of  $k$ .

**Lemma 4.1** (Ogg). *If  $e_p = 1$  or 2 for every prime then  $3|h_k$  (where  $e_p$  is the ramification degree of  $p$  in  $K$  and  $h_k$  is the class number of  $k$ ).*

*Proof.* The ramification index of any prime in  $K$  over  $k$  divides 3, the degree of the extension. So, since  $e_p = 1$  or 2 for every prime in  $K$ , all of the ramification must occur already in  $k$ . Thus  $K$  is an unramified abelian extension of  $k$  and we conclude that it is contained in the maximal unramified abelian extension of  $k$  which has order  $h_k$ . Hence,  $h_k$  is divisible by 3.  $\square$

**Lemma 4.2** (Ogg). *If  $E$  has multiplicative reduction at  $p$  then the ramification degree of  $p$  in  $K = \mathbb{Q}(E[2])$  is 1 or 2.*

*Proof 1* (for  $p \neq 2$ , using only elementary tools). We can pick a Weierstrass equation  $y^2 = f(x)$  as in 4.1 minimal at all primes except 2. Reducing over  $\mathbb{F}_p$ , we get  $\tilde{E} : \tilde{y}^2 = \tilde{f}(x)$ . Now, because the reduction is multiplicative,  $\tilde{E}_{n,s} \cong \mathbb{F}_p^\times$  so since  $-1$  has order 2 in  $\mathbb{F}_p^\times$ , there is a non-singular point of order 2 on  $\tilde{E}$ ,  $(a, 0)$  where  $a$  is a root of  $\tilde{f}$ . Non-singularity implies  $\tilde{f}'(a)$  is non-zero and so this is a simple root in  $\mathbb{F}_p$  which we can lift to a root of  $f$  in  $\mathbb{Q}_p$ . Thus,  $f$  either factors completely or into an irreducible quadratic and a linear factor in  $\mathbb{Q}_p$ . Thus,  $\mathbb{Q}_p(E[2])/\mathbb{Q}_p$  has degree one or two and as all of the ramification must occur in the local extension, we see that the ramification degree of  $p$  divides 2.  $\square$

*Proof 2* (for all  $p$ , from Ogg [14]). , Tate [19] shows that  $(\mathbb{Q}_p)^\times / p^{m\mathbb{Z}}$  is isomorphic to  $E(\mathbb{Q}_p)$ . The image of  $-1$  then gives a point of order 2, so we see that  $K_\varphi$  is a degree 1 or 2 extension of  $\mathbb{Q}_p$  where  $\varphi$  is a prime above  $p$ , and thus the ramification degree is 1 or 2.  $\square$

**Lemma 4.3** (Ogg). *If  $E$  has good reduction at  $p \neq 2$  then  $p$  is unramified in  $K = \mathbb{Q}(E[2])$ .*

*Proof.* By [18, Prop VII.4.1],  $E[2]$  is unramified at  $p$  so  $I_p$  acts trivially on  $\mathbb{Q}_p(E[2])$  thus  $\mathbb{Q}_p(E[2])$  is unramified over  $\mathbb{Q}_p$  so  $\mathbb{Q}(E[2])$  is unramified at  $p$ .  $\square$

Note that the above is really just a specific case of the following result:

**Lemma 4.4.** *If  $E$  has good reduction at  $p$  and  $p \nmid m$  then  $p$  is unramified in  $K = \mathbb{Q}(E[m])$ .*

*Proof.* By [18, Prop VII.4.1],  $E[m]$  is unramified at  $p$  so  $I_p$  acts trivially on  $\mathbb{Q}_p(E[m])$  thus  $\mathbb{Q}_p(E[m])$  is unramified over  $\mathbb{Q}_p$  so  $\mathbb{Q}(E[m])$  is unramified at  $p$ .  $\square$

**Lemma 4.5** (Ogg). *There is no degree 3 Galois extension of  $\mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$ , or  $\mathbb{Q}(\sqrt{-2})$  that is ramified only at the prime above 2.*

*Proof.* Let  $k$  be one of these fields and  $K/k$  a degree 3 Galois extension. By  $\wp$  let us denote the prime above 2 (note  $\wp = (2)$  if  $k = \mathbb{Q}$  and  $\wp^2 = (2)$  otherwise). Note  $k$  has class number 1 and residue field  $\mathbb{F}_2$  at  $\wp$ , and since  $K$  is ramified only at  $\wp$  among finite places,  $K$  has modulus  $\wp^n m_\infty$  where  $m_\infty$  is some set of infinite places. So,  $\text{Gal}_{K/k}$  is some quotient of the ray class group  $Cl_k^{\wp^n m_\infty}$ . Since  $\mathcal{O}_k$  is a principal ideal domain, this is just the elements of  $k$  with  $v_\wp(\alpha) = 0 \pmod{n}$  and  $\alpha \equiv 1 \pmod{\wp^n}$ . Thus there are exactly  $2^s \cdot 2^{n-1}$  classes in  $Cl_k^{\wp^n m_\infty}$  where  $s$  is the number of real places dividing  $m_\infty$  because  $\#\mathcal{O}_k/\wp^n = \phi(2^n) = 2^{n-1}$ . So,  $\text{Gal}_{K/k}$  is a 2-group, contradicting that it has degree 3.  $\square$

#### 4.2. Forcing a rational point of order 2.

**Lemma 4.6.** *Let  $p_1, \dots, p_n$  be distinct odd primes and let  $N = 2 \cdot p_1 \dots p_n$ . Suppose  $E/\mathbb{Q}$  is an elliptic curve of conductor  $N$  with no rational 2-torsion point and let  $k = \mathbb{Q}(\sqrt{\Delta})$  where  $\Delta$  is the discriminant of  $E$ . Then  $3|h_k$  where  $h_k$  is the class number of  $k$ .*

*Proof.* Let  $K = \mathbb{Q}(E[2])$  so that  $K/k$  is cubic. Now, for  $p \neq p_i$ , 2 we have that  $E$  has good reduction at  $p$  so by Lemma 4.3  $p$  is unramified in  $K$ . For  $p = p_i$ , 2,  $E$  has multiplicative reduction at  $p$ , so by Lemma 4.6  $e_p = 1$  or 2. Since all primes have ramification degree 1 or 2, by Lemma 4.1 we obtain  $3|h_k$ .  $\square$

**Lemma 4.7.** *Let  $N = p_1 \dots p_n$  be a product of distinct primes  $p_i \equiv \pm 1 \pmod{8}$ . Suppose  $E/\mathbb{Q}$  is an elliptic curve of conductor  $N$  with no rational 2-torsion point and let  $k = \mathbb{Q}(\sqrt{\Delta})$  where  $\Delta$  is the discriminant of  $E$ . Then  $3|h_k$  where  $h_k$  is the class number of  $k$ .*

*Proof.* Let  $K = \mathbb{Q}(E[2])$  so that  $K/k$  is cubic. As in the proof of Lemma 4.6, for  $p \neq p_i$ , 2 we see that  $p$  is unramified in  $K$  and for  $p = p_i$  we see that  $e_p = 1$  or 2. So, it remains to show that the ramification degree at  $p = 2$  is 1 or 2 before we can apply Lemma 4.1 to finish the proof.

First we suppose  $K/\mathbb{Q}$  is a degree 3 extension. Then we see that for  $p \neq 2$ ,  $K$  is unramified at  $p$  since  $e_p = 1$  or 2 from above but  $e_p|3$  since  $K/\mathbb{Q}$  is Galois. But then  $K$  is a cubic cyclic extension of  $\mathbb{Q}$  ramified only at 2, contradicting Lemma 4.5. So, we conclude  $K/\mathbb{Q}$  is a degree 6 extension. Now, let us enumerate the possible factorizations of (2) in  $K$  with ramification degree greater than 2:

$$\begin{aligned} (2) &= \wp_1^3, f = 2 \\ &\text{or} \\ (2) &= \wp_1^6, f = 1 \\ &\text{or} \\ (2) &= \wp_1^3 \wp_2^3, f = 1 \end{aligned}$$

Where  $f$  is the degree of the residue field extension. Now, we can immediately exclude the bottom two possibilities:  $e_p|(p^f)^j(p^f - 1)$  for some  $j$  and thus for  $p = 2$  and  $f = 1, 3 \nmid e_p$ . So, if we can show that (2) either splits or ramifies in  $k$  then we will be done (if it has ramification degree 2 in  $k$  then it has ramification degree 2 or 6 in  $K$ ).

To that end, let  $m$  be the squarefree part of  $\Delta$ . Then, possibly after renumbering,  $m = \pm p_1 \dots p_l$  for some  $l \leq n$ , and  $k = \mathbb{Q}(\sqrt{m})$ . Then we know  $m \equiv \pm 1 \pmod{8}$ . If  $m \equiv -1 \pmod{8}$  then  $m \equiv 3 \pmod{4}$  and  $2 \nmid \text{disc} k$  so 2 ramifies in  $k$ . If  $m \equiv 1 \pmod{8}$  then  $2 \nmid \text{disc} k$  but (2) splits in  $k$  (see, e.g., [10, pp. 57-58]).  $\square$

**Theorem 4.8.** *Let  $N = p_1 \dots p_n$  be a product of distinct primes such that either  $p_i = 2$  for some  $i$  or  $p_i \equiv \pm 1 \pmod{8}$  for all  $1 \leq i \leq n$  and suppose that for any  $m = \pm p_{i_1} \dots p_{i_l}$ ,  $1 \leq i_1 < i_2 < \dots < i_l \leq n$  the class number of  $\mathbb{Q}(\sqrt{m})$  is not divisible by 3. Then any elliptic curve over  $\mathbb{Q}$  of conductor  $N$  has a rational point of order 2.*

*Proof.* Suppose we have an elliptic curve  $E$  of conductor  $N$  with no rational points of order 2. By either Lemma 4.6 or Lemma 4.7,  $3|h_k$  where  $k = \mathbb{Q}(\sqrt{\Delta})$ . But  $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{m})$  for  $m$  as in the statement of the theorem or  $m = \pm 1$ , and none of these have class number divisible by three, so we obtain a contradiction.  $\square$

## 5. CURVES WITH A RATIONAL POINT OF ORDER 2

Suppose that  $E$  is an elliptic curve with conductor  $N = pq$  for distinct odd primes  $p$  and  $q$  and also that  $E$  has a rational point of order 2. Our initial goal will be to use this curve to produce a solution to some diophantine equation, which we will do by examining the discriminant of a minimal Weierstrass equation for  $E$ . For the initial set up in 5.1 we follow Setzer, *et al.* [17, Sec. 2] closely, though we elaborate on several points in the interest of clarity. Afterwards, in 5.2 we restrict the equations that can arise further using ideas similar to those of Setzer, *et al.* [17, Sec. 2], although the addition of a second prime factor makes the analysis much more complicated. Finally, in 5.3 we show that under certain congruency conditions on  $p$  and  $q$  none of these equations have solutions and therefore there cannot be an elliptic curve of conductor  $N$  with a rational point of order 2.

**5.1. Diophantine Setup .** Consider a minimal model for  $E$ :

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

with discriminant  $\Delta_0 = \pm p^\alpha q^\beta$  where  $1 \leq \alpha, \beta$ . By the change of coordinates

$$y' = \frac{1}{8}(y - a_1x - 4a_3), \quad x' = \frac{1}{4}x$$

this curve is also given by

$$y'^2 = x'^3 + b_2x'^2 + 8b_4x' + 16b_6$$

where the  $b_k$  are the standard invariants

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6 \end{aligned}$$

and the discriminant of this equation is  $2^{12}\Delta_0$ .

Now, since  $2 \nmid N$ , the reduction at 2 must be non-singular, and so, since every Weierstrass model over  $\mathbb{F}_2$  with  $a_1$  and  $a_3$  equal to 0 gives a singular curve, we see that at least one of  $a_1$  and  $a_3$  is odd. Suppose  $a_1$  is even and  $a_3$  is odd. Then,  $4|b_2$ ,  $2|b_4$ , and  $2 \nmid b_6$ . Now, we know that there is a rational point of order 2, and so there is a rational root of the polynomial

$$(5.1) \quad x'^3 + b_2x'^2 + 8b_4x' + 16b_6$$

and in particular there is a root of this polynomial in  $\mathbb{Q}_2$ . However,  $v_2(16b_6) = 4$ ,  $v_2(8b_4) \geq 4$ , and  $v_2(b_2) \geq 2$ , and therefore, by considering the Newton polygon, we conclude that this polynomial has exactly three roots in  $\overline{\mathbb{Q}_2}$  of valuation  $4/3$ , and thus none of these roots lie in  $\mathbb{Q}_2$ , giving us a contradiction. So, we must have that  $a_1$  is odd. This gives us that

$$(5.2) \quad b_2 \equiv 1 \pmod{4}, \quad b_6 \equiv 0 \text{ or } 1 \pmod{4}, \quad \text{and } b_4 \equiv b_6 \pmod{2}$$

Now, let  $t$  be a rational (and thus integral) root of

$$x'^3 + b_2x'^2 + 8b_4x' + 16b_6$$

Then by the substitution  $x' = X + t$  and  $y' = Y + t$  we get a new equation for  $E$

$$(5.3) \quad Y^2 = X^3 + AX^2 + BX$$

where

$$\begin{aligned} A &= b_2 + 3t \\ B &= 3t^2 + 2b_2t + 8b_4 \end{aligned}$$

Now, since  $t$  is a root of [5.1](#), considering the equation mod 8 we see

$$t^3 + b_2t^2 \equiv 0 \pmod{8}$$

and thus  $t \equiv 0$  or  $-b_2 \pmod{8}$ . Now, if  $t \equiv 0 \pmod{8}$ , plugging this in to [5.1](#) we see  $b_6 \equiv 0 \pmod{2}$  and thus  $b_4 \equiv 0 \pmod{2}$  by [5.2](#). So, combining this with the other conditions in [5.2](#) we find  $A \equiv 1 \pmod{4}$  and  $B \equiv 0 \pmod{16}$ . On the other hand, for  $t \equiv -b_2 \pmod{8}$  we obtain  $A \equiv 6 \pmod{8}$  and  $B \equiv 1 \pmod{8}$ , and so we have determined that either:

$$\begin{aligned} A &\equiv 1 \pmod{4} \quad \text{and} \quad B \equiv 0 \pmod{16} \\ &\text{or} \\ A &\equiv 6 \pmod{8} \quad \text{and} \quad B \equiv 1 \pmod{8} \end{aligned}$$

Now, since the change of coordinates we made to obtain [5.3](#) was a translation, the discriminant did not change, and so we conclude

$$16B^2(A^2 - 4B) = 2^{12}\Delta_0$$

so

$$(5.4) \quad B^2(A^2 - 4B) = \pm 2^8 p^\alpha q^\beta$$

Furthermore,  $E$  has multiplicative reduction mod  $p$  and  $q$ , and thus  $Y^2 = X^3 + AX^2 + BX$  has a double root but not a triple root mod  $p$  and mod  $q$  so we conclude that each of  $p$  and  $q$  can divide only one of  $A$  and  $B$ .

Lastly, suppose  $\alpha$  is odd. Then if  $p|B$  we see that  $p|A$  and thus, since  $p$  cannot divide both,  $p \nmid B$ . Similarly if  $\beta$  is odd  $q \nmid B$ .

We conclude that  $E$  gives rise to a solution of Equation [5.4](#) under all of these conditions, which we will summarize below at the start of [5.2](#).

**5.2. Diophantine Solutions .** We have established that  $E$  gives rise to a solution of the following equation:

$$B(A^2 - 4B) = \pm 2^8 p^\alpha q^\beta \text{ where}$$

$$1 \leq \alpha, \beta$$

$p$  and  $q$  each divide at most one of  $A, B$ ,

if  $\alpha$  is odd  $p \nmid A$  and if  $\beta$  is odd  $q \nmid B$ , and

either  $A \equiv 1 \pmod{4}$  and  $B \equiv 0 \pmod{16}$  or  $A \equiv 6 \pmod{8}$  and  $B \equiv 1 \pmod{8}$

To further refine the possibilities, we will break down into cases:

If  $\alpha$  and  $\beta$  are both odd, then  $B = \pm 2^k$  for  $0 \leq k \leq 4$  and we see that, by the congruency conditions on  $B$ ,  $B = 1$  or  $B = \pm 16$ . We consider these cases based on the sign of the right hand side of the equation:

$$\Delta_0 > 0 :$$

- If  $B = 1$  then  $A^2 - 4 = 256p^\alpha q^\beta$ . Letting  $C = A - 2$ ,

$$C(C + 4) = 256p^\alpha q^\beta$$

and since the only prime that can divide both  $C$  and  $C + 4$  is 2 and  $C \equiv 4 \pmod{8}$  we see  $C = 2^2 p^\alpha$  and  $C + 4 = 2^6 q^\beta$ , possibly after swapping  $p$  and  $q$ . And thus  $4 = 2^6 q^\beta - 2^2 p^\alpha$ , so we get  $1 = 2^4 q^\beta - p^\alpha$  or  $1 = 2^4 p^\alpha - q^\beta$ .

- If  $B = 16$  then  $A^2 - 64 = p^\alpha q^\beta$  so  $(A - 8)(A + 8) = p^\alpha q^\beta$  and since the only prime that can divide both  $A - 8$  and  $A + 8$  is 2, we conclude  $|p^\alpha - q^\beta| = 16$ .
- If  $B = -16$  then  $A^2 + 64 = p^\alpha q^\beta$ .

$$\Delta_0 < 0 :$$

- If  $B = 1$  then  $A^2 - 4 = -256p^\alpha q^\beta$  which has no solutions.
- If  $B = 16$  then  $A^2 - 64 = -p^\alpha q^\beta$  so, since we are only considering  $p$  and  $q$  not equal to 2 and we must have  $A \equiv 1 \pmod{4}$ , by enumeration we see the only solutions with  $\alpha$  and  $\beta$  odd are  $(-3)^2 - 64 = -5 \cdot 11$ ,  $5^2 - 64 = -3 \cdot 13$ , and  $(-7)^2 - 64 = -3 \cdot 5$ .
- If  $B = -16$  then  $A^2 + 64 = -p^\alpha q^\beta$ , which has no solutions.

If  $\alpha$  is odd and  $\beta$  is even, then  $B = \pm 2^k q^b$  and in fact we see  $b = \beta/2$  or 0 because otherwise  $q$  divides both  $A$  and  $B$ . By the congruency conditions we see that either  $B = \pm 16$ ,  $B = 1$ ,  $B = \pm 16q^{\beta/2}$ , or  $B = \pm q^{\beta/2}$  (the last occurring only when  $\pm q^{\beta/2} \equiv 1 \pmod{8}$ ). We consider these cases based on the sign of the right hand side of the equation:

$$\Delta_0 > 0 :$$

- If  $B = 1, \pm 16$ , we obtain the same equations as above in the case of  $\alpha$  and  $\beta$  both odd except we add a solution to the case  $A^2 - 64 = -p^\alpha q^\beta$  with  $1^2 - 64 = -3^2 \cdot 7$ .
- If  $B = 16q^{\beta/2}$ , then  $A^2 - 64q^{\beta/2} = p^\alpha$ .
- If  $B = -16q^{\beta/2}$ , then  $A^2 + 64q^{\beta/2} = p^\alpha$ .
- If  $B = q^{\beta/2}$  then  $A^2 - 4q^{\beta/2} = 256p^\alpha$ .
- If  $B = -q^{\beta/2}$  then  $A^2 + 4q^{\beta/2} = 256p^\alpha$ .

$$\Delta_0 < 0 :$$

- If  $B = 1, \pm 16$ , we obtain the same equations as above in the case of  $\alpha$  and  $\beta$  both even.
- The rest are as with  $\Delta_0 > 0$ , but with negatives on the right hand side.

If  $\alpha$  is even and  $\beta$  is odd, then this is equivalent to the above case with  $p$  and  $q$  swapped. If both  $\alpha$  and  $\beta$  are even then  $B = \pm 2^k p^a$  or  $B = \pm 2^k q^b$  where again we see that  $a = \alpha/2$  or  $0$  and  $b = \beta/2$  or  $0$  because otherwise  $p$  or  $q$  would divide both  $A$  and  $B$ . So, we reduce to the same equations as for  $\alpha$  odd and  $\beta$  even or vice versa.

In summary, we have proven the following:

**Theorem 5.1.** *If there is an elliptic curve of conductor  $N = pq$  and minimal discriminant  $\pm p^\alpha q^\beta$  with a rational point of order 2 for  $p$  and  $q$  odd primes, and  $pq$  is not one of 15, 21, 39, and 55, then one of the following diophantine equations has a solution:*

Equations	$\alpha$ and $\beta$ values ( $1 \leq \alpha, \beta$ )
(1) $1 = 2^4 q^\beta - p^\alpha$ or $1 = 2^4 p^\alpha - q^\beta$	all
(2) $ p^\alpha - q^\beta  = 16$	all
(3) $A^2 + 64 = p^\alpha q^\beta$	all
(4a) $A^2 \pm 64q^{\beta/2} = \pm p^\alpha$	$\beta$ even, all $\alpha$
(5a) $A^2 - 4q^{\beta/2} = \pm 256p^\alpha$ ,	$\beta$ even and $q^{\beta/2} \equiv 1 \pmod{8}$ , all $\alpha$
(6a) $A^2 + 4q^{\beta/2} = \pm 256p^\alpha$	$\beta$ even and $q^{\beta/2} \equiv -1 \pmod{8}$ , all $\alpha$
(4b) $A^2 \pm 64p^{\alpha/2} = \pm q^\beta$	$\alpha$ even, all $\beta$
(5b) $A^2 - 4p^{\alpha/2} = \pm 256q^\beta$	$\alpha$ even and $p^{\alpha/2} \equiv 1 \pmod{8}$ , all $\beta$
(6b) $A^2 + 4p^{\alpha/2} = \pm 256q^\beta$	$\alpha$ even and $p^{\alpha/2} \equiv -1 \pmod{8}$ , all $\beta$

### 5.3. Non-existence of curves with a rational point of order 2.

**Proposition 5.2.** *Suppose  $p$  and  $q$  are distinct primes such that  $p, q \equiv 1 \pmod{3}$ ,  $p, q \equiv 1 \pmod{5}$  and  $p, q \equiv 3 \pmod{4}$  but  $p \notin \langle q \rangle$  where  $\langle q \rangle$  is the subgroup generated by  $q$  in  $(\mathbb{Z}/16\mathbb{Z})^\times$ . Then there is no elliptic curve of conductor  $pq$  with a rational point of order 2.*

*Proof.* By Theorem 5.1 it suffices to show that there is no solution to any of the diophantine equations listed in the table therein.

From the equations in (1), we obtain  $1 \equiv 0 \pmod{3}$ , a contradiction.

From the equations in (2), we obtain  $p^\alpha \equiv q^\beta \pmod{16}$ . With our conditions on  $p, q \pmod{16}$ , this can only happen when  $\alpha$  and  $\beta$  are both even. So, if  $p^\alpha > q^\beta$ , we obtain

$$p^\alpha = 16 + q^\beta = (4 + i \cdot q^{\beta/2})(4 - i \cdot q^{\beta/2})$$

and so we see that since  $p$  is prime in  $\mathbb{Q}(i)$  ( $p \equiv 3 \pmod{4}$ ), both of  $4 \pm i \cdot q^{\beta/2}$  are powers of  $p$ , which clearly cannot be. We obtain a similar contradiction if  $q^\beta > p^\alpha$ .

From equation (3), we obtain

$$(A + 8i)(A - 8i) = p^\alpha q^\beta$$

but since  $p \equiv 3 \pmod{4}$  it is prime in  $\mathbb{Q}(i)$  and thus since clearly it cannot divide both  $A + 8i$  and  $A - 8i$ , one of them is equal to  $p^\alpha$ . But then the other is equal to  $q^\beta$  and in particular they are both rational integers, which cannot be.

From the equations in  $(4a/b)$ ,  $(5a/b)$ , and  $(6a/b)$ , we obtain either that a positive number is equal to a negative number, that 2 is a square mod 3, or that 2 or 3 is a square mod 5, all of which give contradictions.  $\square$

## 6. NON-EXISTENCE OF ELLIPTIC CURVES WITH CERTAIN CONDUCTORS $pq$

Here we combine the results of the two previous sections to prove a general nonexistence result on elliptic curves of conductor  $N = pq$  for certain  $p, q$ .

**Theorem 6.1.** *Suppose  $p$  and  $q$  are distinct primes such that  $p \equiv 7 \pmod{16}$ ,  $q \equiv 15 \pmod{16}$ , and  $p, q \equiv 1 \pmod{15}$ . Suppose furthermore that none of the class numbers of  $\mathbb{Q}(\sqrt{\pm p})$ ,  $\mathbb{Q}(\sqrt{\pm q})$ , and  $\mathbb{Q}(\sqrt{\pm pq})$  are divisible by 3. Then there are no elliptic curves of conductor  $pq$ .*

*Proof.* By Theorem 4.8, any such curve will have a rational point of order 2, but by Proposition 5.2 there is no such curve with a rational point of order 2.  $\square$

The following table lists all 67 of the  $N = pq$  less than  $10^7$  to which Theorem 6.1 applies. In particular, we note that only one of these is less than 130000 and thus the rest are not contained in John Cremona's tables [5]. The source code for the SAGE program we used to find these is contained in Section 8.

N	p	q
40921	151	271
149641	151	991
171001	631	271
403321	151	2671
496201	1831	271
548281	151	3631
625321	631	991
626281	2311	271
691321	2551	271
693241	151	4591
928201	631	1471
951481	3511	271
1055641	151	6991
1454281	151	9631
1635481	151	10831
1671721	151	11071
1685401	631	2671
1814521	1831	991
1889161	151	12511
2179081	151	14431
2252281	8311	271
2432761	151	16111
2528041	2551	991
2650201	151	17551
2693401	1831	1471

3338761	151	22111
3479401	3511	991
3748201	13831	271
3752521	2551	1471
3943321	14551	271
4172281	151	27631
4317241	151	28591
4715881	151	31231
4890601	1831	2671
4906441	4951	991
5164681	3511	1471
5331961	151	35311
5730601	151	37951
5803081	151	38431
5925721	631	9391
6077161	631	9631
6095641	6151	991
6172681	2311	2671
6349801	23431	271
6414841	23671	271
6648361	1831	3631
6813721	2551	2671
6985801	631	11071
6999001	151	46351
7071481	151	46831
7390441	27271	271
7780681	28711	271
7832521	151	51871
8122441	151	53791
8235961	30391	271
8267401	151	54751
8406121	1831	4591
8412361	151	55711
8651641	631	13711
8774761	151	58111
9105961	631	14431
9262681	2551	3631
9341641	34471	271
9377881	3511	2671
9572041	151	63391
9666841	35671	271
9731881	35911	271

## 7. FUTURE WORK

There are some obvious avenues to explore in future work:

- We could further examine the Diophantine equations given by Theorem 5.1 in order to find more conditions beyond just those of Proposition 5.2 under which they have no solutions. In particular, it would be useful to have a result such as the one by Hadano which we restated in Theorem 3.8, that is to say a result that under certain conditions allows us to bound the exponents appearing in the equations of Theorem 5.1 so that we can reduce to checking for solutions of only finitely many equations. We note here that we have some weak evidence that this may be possible: by examining the data in Cremona's tables [5] we find that there is only one conductor  $N = pq < 130000$  for  $p$  and  $q$  odd primes such that there is an elliptic curve of conductor  $N$  with a rational point of order 2 but no solution to one of these diophantine equations for exponents  $< 12$  (this is  $N = 3 \cdot 33937$ , for which we have to go up to discriminant  $3^{26} \cdot 33937$ ).
- We could try to extend the results of Edixhoven, *et al.* [8] in order to show that for some of the  $p$  and  $q$  to which our results apply there are also no curves with additive reduction at  $p$  and/or  $q$ .
- We could investigate the conditions under which quadratic fields will have class number three in order to at least give a conjecture or heuristic argument on the density of conductors  $N$  to which Theorem 6.1 should apply. There is a reasonable amount of literature on class number divisibility that we have yet to examine.

## 8. SOURCE CODE

Here we present the source code for the SAGE program that we used to find all  $N = pq < 10^7$  to which Theorem 6.1 applies (the table of these  $N$  follows Theorem 6.1). We note that we were able to run this search on a small netbook computer in around 15 minutes, and so it would certainly be possible to go up to a much higher number.

```
% Search up to R for prime pairs satisfying
% the congruency conditions
R=10000000;
L=[];
for p in prime_range(3,R):
    if (mod(p,15)==1) and (mod(p,16)==7):
        for q in prime_range(3,R/p):

            if (mod(q,15)==1) and (mod(q,16)==15):
                L.append((p,q));
% List the primes occurring in the prime pairs
P=[];
for pair in L:
    if not (pair[0] in P):
        P.append(pair[0]);
    if not (pair[1] in P):
        P.append(pair[1]);
% Find the primes that satisfy the class number conditions
GoodPrimes=[];
for p in P:
```

```

pos=QuadraticField(p,'x').class_number();
neg=QuadraticField(-p,'x').class_number();
if (not (mod(pos,3)==0)) and (not (mod(neg,3)==0)):
    GoodPrimes.append(p);
% Find the pairs that satisfy the class number conditions
% Output GoodPairs will be our final list
GoodPairs=[];
for pair in L:
    p=pair[0];
    q=pair[1];
    if (p in GoodPrimes) and (q in GoodPrimes):
        n=p*q;
        pos=QuadraticField(n,'x').class_number();
        neg=QuadraticField(-n,'x').class_number();
        if (not (mod(pos,3)==0)) and (not (mod(neg,3)==0)):
            GoodPairs.append((n,p,q));

```

## REFERENCES

- [1] M. K. Agrawal, J. H. Coates, D. C. Hunt, and A.J. van der Poorten. Elliptic curves of conductor 11. *Mathematics of Computation*, 35(151):991–1002, July 1980.
- [2] B. J. Birch and W. Kuyk, editors. *Modular Functions of One Variable IV*. Lecture Notes in Mathematics. Springer-Verlag, 1975.
- [3] Nigel Boston. A refinement of the Faltings-Serre method. *London Math. Soc. Lecture Note Ser.*, 215:61–68, 1995.
- [4] Arnand Brumer and Kenneth Kramer. The rank of elliptic curves. *Duke Math. J.*, 44(4):715–743, 1977.
- [5] John Cremona. Elliptic curve data. <http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/>.
- [6] John Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, 1992.
- [7] Henri Darmon. A proof of the full Shimura-Taniyama-Weil conjecture is announced. *Notices Ameri. Math. Soc.*, 46(11):1397–401, 1999.
- [8] Bas Edixhoven, Arnold de Groot, and Jaap Top. Elliptic curves over the rationals with bad reduction at only one prime. *Mathematics of Computation*, 54(189):413–419, January 1990.
- [9] Toshihiro Hadano. On the conductor of an elliptic curve with a rational point of order 2. *Nagoya Math J.*, 53:199–210, 1974.
- [10] James S. Milne. *Algebraic Number Theory (v 3.02)*. 2009. Available at [www.jmilne.org/math/](http://www.jmilne.org/math/).
- [11] I. Miyawaki. Elliptic curves of prime power conductor with  $\mathbb{Q}$ -rational points of finite order. *Osaka J. Math.*, 10:309–323, 1973.
- [12] L. J. Mordell. *Diophantine Equations*. Academic Press London and New York, 1969.
- [13] Olaf Neumann. Elliptische kurven mit vorgeschriebenem reduktionsverhalten. ii. *Math. Nachr.*, 56:269–280, 1973.
- [14] A. P. Ogg. Abelian curves of 2-power conductor. *Proc. Camb. Phil. Soc.*, 62:143–148, 1966.
- [15] A. P. Ogg. Abelian curves of small conductor. *J. reine und angew Math.*, 226:204–215, 1967.
- [16] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15:259–331, 1972.
- [17] Bennett Setzer. Elliptic curves of prime conductor. *J. London Math. Soc.*, 10:367–378, 1975.
- [18] Joseph Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.
- [19] John Tate. A review of non-Archimedean elliptic functions. In *Elliptic Curves, Modular Forms, & Fermat's Last Theorem*, 1997.
- [20] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math.*, 141:443–551, 1995.