Simultaneous twists of elliptic curves and the Hasse principle for certain K3 surfaces

Vivek Pal

Submitted in partial fulfillment of the
requirements for the degree
of Doctor of Philosophy
in the Graduate School of Arts and Sciences

COLUMBIA UNIVERSITY

2016

ABSTRACT

Simultaneous twists of elliptic curves and the Hasse principle for certain K3 surfaces

Vivek Pal

In this thesis we unconditionally show that certain K3 surfaces satisfy the Hasse principle. Our method involves the 2-Selmer groups of simultaneous quadratic twists of two elliptic curves, only with places of good or additive reduction. More generally we prove that, given finitely many such elliptic curves defined over a number field (with rational 2-torsion and satisfying some mild conditions) there exists an explicit quadratic extension such that the quadratic twist of each elliptic curve has essential 2-Selmer rank one. Furthermore, given a 2-covering in each of the 2-Selmer groups, the quadratic extension above can be chosen so that the 2-Selmer group of the quadratic twist of each elliptic curve is generated by the given 2-covering and the image of the 2-torsion.

Our approach to the Hasse Principle is outlined below and was introduced by Skorobogatov and Swinnerton-Dyer in [Skorobogatov and Swinnerton-Dyer, 2005]. We also generalize the result proved in [Skorobogatov and Swinnerton-Dyer, 2005]. If each elliptic curve has a distinct multiplicative place of bad reduction, then we find a quadratic extension such that the quadratic twist of each elliptic curve has essential 2-Selmer rank one. Furthermore, given a 2-covering in each of the 2-Selmer groups, the quadratic extension above can be chosen so that the 2-Selmer group of the quadratic twist of each elliptic curve is generated by the given 2-covering and the image of the 2-torsion. If we further assume the finiteness of the Shafarevich-Tate groups (of the twisted elliptic curves) then each elliptic curve has Mordell-Weil rank one. If $K = \mathbb{Q}$, then under the above assumptions the analytic rank of each elliptic curves is one. Furthermore, with the assumption on the Shafarevich-Tate group (and $K = \mathbb{Q}$), we describe a single quadratic twist such that each elliptic curve has analytic rank zero and Mordell-Weil rank zero, again under some mild assumptions.

Table of Contents

Acknowledgments

I would like to thank my advisor Wei Zhang, he has been a great advisor and a friend. Wei has always been very supportive and I really appreciate all the time he spent working with me. I have learned a lot from Wei, he has remarkable insight, in particular his suggestion to work on this project.

The Columbia Mathematics department has been amazing! The faculty are so friendly and approachable, it makes for a great atmosphere. In particular I would like to thank Johan de Jong, Davesh Maulik and Andrei Okounkov for great discussions, both mathematical and otherwise. Attending, organizing and giving talks in the seminars here has been very helpful for me - it has helped me develop skills that I will continue to use in the future.

Special thanks to my committee members, Dorian Goldfeld, Eric Urban, Johan de Jong and Gautam Chinta - for everything!

I would like to thank all my friends in New York, having them around has made my time at Columbia so much more enjoyable. In particular I would like to thank my closest friends, Karsten Gimre, João Guerreiro, Connor Mooney, and Andrey Smirnov - exploring New York City with them has been so much fun!

Most importantly I would like to thank my family: my mom, my sisters, Pankaj and Priya and my brother, Suchandan. My mom has been so amazing and strong, she is an inspiration! My siblings are truly the best! They are always there when I need something and I could not have done this without them. Pankaj, as my oldest sibling, has always set the bar really high and has shown me that anything is possible. Priya's dedication to her projects and amazing work ethic are inspiring, her energy is simply contagious! Discussions with Chandan, both about math and other topics, have always been enlightening - he has such deep and well thought out responses, it's unbelievable. I have really benefited from bouncing ideas off of him.

Last, but not least I would like to thank the staff in the Columbia Math department, they

helped make everything run smoothly. The support the department has given me, has allowed me to attend many conferences that have really helped me academically. In particular I would like to thank Terrance Cope and Mary Young, they both spoiled us before retiring.

To my family

Part I

The Hasse Principle, unconditionally

Chapter 1

Introduction

The Hasse principle claims that if a variety X, defined over a number field K, has points over every completion of K, i.e. $X(K_v) \neq 0$ for all places v of K, then X has points over K, i.e $X(K) \neq 0$. The Hasse-Minkowski theorem shows that the Hasse principle holds for quadratic forms. In general there are many obstructions to the Hasse Principle, for example the Bauer-Manin obstruction. It is believed that, for K3 surfaces, the Brauer-Manin obstruction is the only obstruction to the Hasse principle, see [Skorobogatov and Zarhin, 2008]. There are many conditional results in this direction, for example see [Skorobogatov and Swinnerton-Dyer, 2005]. The goal of this article is to *unconditionally* prove the Hasse principle for some K3 surfaces. In Theorem 1.1.2, we describe a family of K3 surfaces that unconditionally satisfy the Hasse principle.

Let $Y = C_1 \times C_2$ be a 2-covering (e.g. see [Cremona, 2001]) of a product of two elliptic curves, $E^1 \times E^2$ defined over a number field K. Let X be the smooth projective desingularization of Y modulo the Kummer involution on C_i. The Hasse principle for X assumes that it has points over each completion of K and asks if X has points over K. Under the assumption that the Shafarevich-Tate group (of some quadratic twist) of both E^i is finite and other technical conditions, this question was answered by A. Skorobogatov and P. Swinnerton-Dyer in [Skorobogatov and Swinnerton-Dyer, 2005]. We prove a more general conditional result below, see Theorem 9.0.15.

A simpler question to ask is, if Y has local solutions for all completions of K then does X have a global solution? This is a weaker version of the Hasse principle, since if Y is everywhere locally soluble then X is as well, but not necessarily vice versa. In this article we prove an unconditional result showing that for certain Y, if Y is everywhere locally soluble then X has a global solution.

One instance of this is the explicit example in Theorem 1.1.1 and a more general version is outlined in Chapter 6.

Our approach to the Hasse Principle is outlined below and was introduced by Skorobogatov and Swinnerton-Dyer in [Skorobogatov and Swinnerton-Dyer, 2005]. Their method is based on simultaneous quadratic twists of two elliptic curves. The results on quadratic twists stated here are proved using cohomological methods; this allows us to work with finitely many elliptic curves and with more general types of bad reduction. We are also able to use a result of Tian-Yuan-Zhang to unconditionally prove the Hasse principle for certain K3 surfaces, see Theorem 1.1.2. For a more general example see the end of Chapter 6. The unconditional result requires twisting elliptic curves with complex multiplication, in particular elliptic curves with no multiplicative place.

1.1 Summary of results

Let K be a number field, E be an elliptic curve and let $\mathrm{Sel}_2(E/K)$ denote the 2-Selmer group of E over K. Given finitely many elliptic curves with rational 2-torsion (i.e. $E[2] \subset E(K)$), satisfying some mild hypotheses, we find a single quadratic twist such that the twisted elliptic curves each have 2-Selmer rank equal to two or three. Hence they each have Mordell-Weil rank zero and the 2-torsion part of their Shafarevich-Tate group is trivial. Furthermore, there are infinitely many such quadratic twists since the described twist is given by congruence conditions.

Let $g(d)$ be the genus class number, i.e. the order of two times the class group of $\mathbb{Q}(\sqrt{-d})$. The parity of $g(n)$ can be explicitly computed using Rédei matrices, see Chapter 6. As an application of these results we show that a family of K3 surfaces unconditionally satisfies an approximation to the Hasse Principle and a subset satisfies the Hasse Principle:

Theorem 1.1.1. *Let m, n be integers and $p, q \equiv 3 \mod 4$ prime numbers such that $p|n$, $q|m$, $p \nmid m$, $q \nmid n$, $\gcd(n/p, m) \neq n/p$ and $\gcd(m/q, n) \neq m/q$. Suppose both n and m satisfy one of the following conditions:*

- *$n \equiv 5 \mod 8$ such that $g(n)$ is odd and all but one of the prime factors of n are $\pm 1 \mod 8$ and one is $5 \mod 8$*
- *$n \equiv 7 \mod 8$ such that $g(n)$ is odd and all but one of the prime factors of n are $\pm 3 \mod 8$ and one is $7 \mod 8$*

If both $Z_1^2 = (p - \frac{n^2}{p}X^4)$ *and* $Z_2^2 = (q - \frac{m^2}{q}Y^4)$ *are everywhere locally soluble, then*

$$Z^2 = \left(p - \frac{n^2}{p}X^4\right)\left(q - \frac{m^2}{q}Y^4\right), \tag{1.1}$$

has a solution in $\mathbb{Q}$.

For the proof of Theorem 1.1.1 see Chapter 6.2.

Let $\left(\frac{\cdot}{\cdot}\right)$ be the Legendre symbol. Given a prime p dividing n, we say the pair (n, p) satisfies $P(n, p)$ if it satisfies the three conditions:

$$1.\ \left(\frac{p}{q}\right) = 1\ \forall q | n, q \neq p \quad 2.\ \left(\frac{2}{p}\right) = 1 \ \text{ and } \quad 3.\ \left(\frac{n/p}{p}\right) = 1.$$

Theorem 1.1.2. *Let* $m, n, p, q \in \mathbb{Z}$ *be as in Theorem 1.1.1. If* (n, p) *satisfies* $P(n, p)$ *and* (m, q) *satisfies* $P(m, q)$*, then*

$$Z^2 = \left(p - \frac{n^2}{p}X^4\right)\left(q - \frac{m^2}{q}Y^4\right), \tag{1.2}$$

satisfies the Hasse Principle, i.e. it has a solution in $\mathbb{Q}$.

For the proof of Theorem 1.1.2 see Chapter 6.2.

In order to state our our main theorems in terms of quadratic twists of elliptic curves, we introduce some definitions.

Definition 1.1.3. Let E be an elliptic curve over a number field K. The essential 2-Selmer rank of E is

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E/K) - \dim_{\mathbb{F}_2} E[2](K).$$

Definition 1.1.4. Let $E^1, \ldots, E^n$ be elliptic curves over K. Then a place, v, of K is a distinct place of bad (additive, multiplicative) reduction for E^i if v is a place of bad (additive, multiplicative) reduction for E^i and a place of good reduction for all E^j, $j \neq i$.

For an elliptic curve E over K and a quadratic extension F/K, the quadratic twist of E by F is denoted by E^F or if $F = K(\sqrt{b})$ then by E_b.

Given finitely many elliptic curves and an element of the 2-Selmer group (an everywhere locally soluble 2-covering) for each elliptic curve, we describe sufficient conditions to find a single quadratic twist such that the 2-Selmer groups of the twisted elliptic curves are 3-dimensional (generated by the 2-covering and the image of the 2-torsion).

We now briefly describe an application of the above result to the Hasse principle for K3 surfaces. This method was introduced by Skorobogatov and Swinnerton-Dyer, [Skorobogatov and Swinnerton-Dyer, 2005]. Consider the K3 surface defined by:

$$Z^2 = f(X)g(Y), \tag{1.3}$$

where $f(X)$ and $g(Y)$ are quartic polynomials with no repeated roots. We are interested in showing that under some conditions the K3 surface above satisfies the Hasse principle.

A solution to equation (1.3) is equivalent to a solution to both

$$D_a^1 : Z_1^2 = af(X) \text{ and } D_a^2 : Z_2^2 = ag(Y), \tag{1.4}$$

for some $a \in K^\times$. The 2-covering D_a^i is a quadratic twist of the 2-covering $D^i := D_1^i$, for $i = 1, 2$. Furthermore, the surface (1.3) is everywhere locally soluble if and only if for each place, v, of K there exists an $a_v \in K_v^\times$ such that both $Z_1^2 = a_v f(X)$ and $Z_2^2 = a_v g(Y)$ have solutions in K_v. Assuming that (1.3) is everywhere locally soluble, the Hasse principle is equivalent to finding an $a \in K^\times$ such that (1.4) has a solution in K.

Let E^1 and E^2 denote the Jacobians of D^1 and D^2, these are elliptic curves since f and g are quartics. We assume that E^1 and E^2 have K-rational 2-torsion, see Theorem 6.0.7.

The general idea will be to find an $a \in K$ such that both D_a^i are everywhere locally soluble. Then D_a^i is an element of $\mathrm{Sel}_2(E_a^i)$, for $i = 1, 2$. We would then like to find a $b \in K^\times$ such that $D_{ab}^i \in \mathrm{Sel}_2(E_{ab}^i)$ and $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_{ab}^i) = 3$, for $i = 1, 2$. Therefore, if we further assume the finiteness of the Shafarevich-Tate group of E_{ab}^i, $i = 1, 2$, then $Ш(E_{ab}^i/K)[2] = 0$. Thus D_{ab}^i are trivial in the Shafarevich-Tate group and hence have global points. This process is described in more detail in Chapter 5.

Chapter 2

Preliminaries

Let K be a number field. For $i = 1, \ldots, n$ let

$$E^i : y^2 = (x - c_1^i)(x - c_2^i)(x - c_3^i)$$

be an elliptic curve with rational 2-torsion, i.e. $c_1^i, c_2^i, c_3^i \in K$. For an elliptic curve, E, let Δ_E denote the discriminant of an integral model of E. Let S_0 be the set of places of K consisting of the set of infinite primes, even primes and a set of generators of the ideal class group of K. Let $S(E)$ denote the set of places of bad reduction of E together with all the places in S_0. Throughout this article, S will denote a finite set of places of K. If v is a place of K then let $\mathcal{O}_{K_v}$ be the ring of integers of K_v, the completion of K at v, and let $\mathcal{O}_{K_v}^\times$ be the units in $\mathcal{O}_{K_v}$.

Let $\left(\frac{\cdot}{\mathfrak{p}}\right) : \mathcal{O}_{K_\mathfrak{p}}^\times \to \{\pm 1\}$ denote the quadratic residue character for the completion of K at an odd prime $\mathfrak{p}$. Note that if $\mathfrak{p} = (\pi)$ then $\left(\frac{\cdot}{\mathfrak{p}}\right) = (\cdot, \pi)_\mathfrak{p}$, where the right hand side is the Hilbert symbol. The equations is independent of the choice of uniformizer since $(\cdot, u\pi)_\mathfrak{p} = (\cdot, u)_\mathfrak{p}(\cdot, \pi)_\mathfrak{p} = (\cdot, \pi)_\mathfrak{p}$.

The p-selmer group of an elliptic curve can be describe in many ways. For example in terms of group cohomology it is given by $\mathrm{Sel}_p(E/K) = \{c \in H^1(K, E[p]) \,|\, \forall v \ \mathrm{loc}_v(c) \in H^1_f(K_v, E[p])\}$, where $H^1_f(K_v, E[p])$ is the image of the local Kummer map and loc_v is the restriction map, for more details see [Silverman, 2009]. For a finite set of places of K, T, let S^T denote the relaxed 2-Selmer group (i.e. $\mathrm{loc}_v(c) \in H^1(K_v, E[2])$ for $v \in T$) and S_T the strict 2-Selmer group (i.e. $\mathrm{loc}_v(c) = 0$ for $v \in T$).

For simplicity, let $d_2(E/K)$ denote the $\mathbb{F}_2$-dimension of the vector space $\mathrm{Sel}_2(E/K)$.

For an elliptic curve with rational 2-torsion (i.e. $E[2] \subset E(K)$) the 2-Selmer group can be

naturally identified with a subspace of $(K^\times/K^{\times 2})^3$, see [Silverman, 2009, Chapter X].

The 2-torsion points of an elliptic curve naturally live in its 2-Selmer group. For an elliptic curve with rational 2-torsion, such as E^i, the image of the 2-torsion elements in the 2-Selmer group is given by:

$$\begin{aligned}&((c_1^i - c_2^i)(c_1^i - c_3^i), (c_1^i - c_2^i), (c_1^i - c_3^i))\\ &((c_2^i - c_1^i), (c_2^i - c_1^i)(c_2^i - c_3^i), (c_2^i - c_3^i))\\ &((c_3^i - c_1^i), (c_3^i - c_2^i), (c_3^i - c_1^i)(c_3^i - c_2^i))\end{aligned} \tag{2.1}$$

Definition 2.0.5. [Skorobogatov and Swinnerton-Dyer, 2005, pg 468] Let E be an elliptic curve with rational 2-torsion and let E_b be a quadratic twist of E, then the restricted 2-Selmer group of E_b is $\{c = (c_1, c_2, c_3) \in \mathrm{Sel}_2(E_b/K) | \forall v \text{ if } \mathrm{val}_v(b) > 0 \text{ then } \mathrm{val}_v(c_i) = 0, i = 1, 2, 3\}$ where val_v is the valuation associated to the place v.

Remark 2.0.6. For $u \in \mathrm{Sel}_2(E/K)$ and a odd prime $\mathfrak{p}$, we say that $\mathfrak{p}$ divides u if one of the components of u has positive valuation at $\mathfrak{p}$. Furthermore, if $b \in K^\times$ then we say a prime $\mathfrak{p}$ divides b if b has positive valuation at $\mathfrak{p}$.

2.1 General lemmas

We will use the next proposition to precisely change the 2-Selmer rank of an elliptic curve under a quadratic twist. This proposition generalizes Proposition 3.3 from [Mazur and Rubin, 2010].

Proposition 2.1.1. *Let E/K be an elliptic curve over K and let T be a set of places of K. Let F/K be a quadratic extension. Let $V_T = \mathrm{loc}_T(\mathrm{Sel}_2(E/K)) \subset \sum_{v\in T} H^1_f(K_v, E[2])$ and $V_T^F = \mathrm{loc}_T(\mathrm{Sel}_2(E^F/K)) \subset \sum_{v\in T} H^1_f(K_v, E^F[2])$, where $\mathrm{loc}_T = \oplus_{v\in T}\mathrm{loc}_v$. If $H^1_f(K_v, E[2]) = H^1_f(K_v, E^F[2])$ for $v \notin T$ and $H^1_f(K_v, E[2]) \cap H^1_f(K_v, E^F[2]) = 0$ for $v \in T$. Then,*

$$\dim \mathrm{Sel}_2(E^F/K) = \dim \mathrm{Sel}_2(E/K) - \dim V_T + \dim V_T^F,$$

with

$$\dim V_T + \dim V_T^F \leq \sum_{v\in T} \dim H^1_f(K_v, E[2]). \tag{2.2}$$

Or more generally,

$$\dim V_T + \dim V_T^F \leq \sum_{v\in T} \dim H^1_f(K_v, E[2]) + \dim[(V_T \cap V_T^F)/S_T].$$

Proof. The proof is a direct generalization of the proof given in [Mazur and Rubin, 2010] and follows from Poitou-Tate duality. □

Lemma 2.1.2. *Let $\mathfrak{q}_0, \mathfrak{q}_1$ be places of additive reduction for E not lying above 2 or 3. Let $\mathfrak{p} = (\pi)$ be a prime ideal not in $S(E)$ such that $\pi \in {K_v^\times}^2$ for all $v \in S(E), v \neq \mathfrak{q}_0, \mathfrak{q}_1$ and $\left(\frac{\pi}{\mathfrak{q}_0}\right) = -1 = \left(\frac{\pi}{\mathfrak{q}_1}\right)$. Then $d_2(E/K) \equiv d_2(E_\pi/K) \mod 2$.*

Proof. The parity of $d_2(E/K) + d_2(E_\pi/K)$ is equal to the parity of the rank of the 2-Selmer group of E over $K(\sqrt{\pi})$ [Monsky, 1996, Lemma 1.2]. The parity of this rank is the same as the parity of the sum $\sum i_v(E/K(\sqrt{\pi}))$ [Kramer, 1981, Theorem 1], where the $i_v(E/K(\sqrt{\pi}))$ is the local norm index as defined in [Kramer, 1981].

By the Kramer-Tunnel conjecture, proved by Kramer-Tunnel and Tim and Vladimir Dokchister in characteristic zero [Dokchitser and Dokchitser, 2011], says:

$$w(E/K_v(\sqrt{\pi}))w(E_\pi/K_v(\sqrt{\pi}))(-\Delta_E, \pi)_v = (-1)^{i_v(E/K(\sqrt{\pi}))}.$$

At all places $v \in S(E)\backslash\{\mathfrak{q}_0, \mathfrak{q}_1\}$ we know that the elliptic curves E and E_π are isomorphic over K_v so the root numbers are the same. Hence $(-\Delta_E, \pi)_v = 1$, since π is locally a square there and thus $i_v(E/K(\sqrt{\pi})) = 0$.

At the places $v = \mathfrak{q}_0, \mathfrak{q}_1$ we use Rohrlich's formula, [Rohrlich, 1996, Theorem 2], to compute the root numbers. It shows that $w(E/K_{\mathfrak{q}_0}(\sqrt{\pi})) = w(E_\pi/K_{\mathfrak{q}_0}(\sqrt{\pi}))$ and similarly for $\mathfrak{q}_1$. Hence $(-\Delta_E, \pi)_{\mathfrak{q}_0} = -1$, since π is locally not a square there and thus $i_{\mathfrak{q}_0}(E/K(\sqrt{\pi})) = 1$. Similarly, at $\mathfrak{q}_1$ we get $i_{\mathfrak{q}_1}(E/K(\sqrt{\pi})) = 1$.

At the place $v = \mathfrak{p}$, the local norm index is given in [Kramer, 1981, Proposition 3], it is $(\Delta_E, \pi)_\mathfrak{p} = (-1)^{i_\mathfrak{p}(E/K(\sqrt{\pi}))}$. Since $(\Delta_E, \pi)_\mathfrak{p} = (\Delta_E, \pi)_{\mathfrak{q}_0}(\Delta_E, \pi)_{\mathfrak{q}_1} = 1$ by the Hilbert Product formula, we see that $i_\mathfrak{p}(E/K(\sqrt{\pi})) = 0$.

Therefore the sum over all places, of the local norm index, is zero. Hence the parity of the 2-Selmer ranks is the same. □

2.2 Elliptic curves with K-rational 2-torsion

Lemma 2.2.1. *[Skorobogatov and Swinnerton-Dyer, 2005, Lemma 4] Let $E : y^2 = (x - c_1)(x - c_2)(x - c_3)$ be an elliptic curve with rational 2-torsion, i.e. $c_1, c_2, c_3 \in K$. Let $\mathfrak{q}$ be an odd prime of*

K, then we describe the image of the local Kummer map, i.e. $H^1_f(K_v, E[2])$.

1. *If $\mathfrak{q}$ divides all the $c_i - c_j$ to the same even power, then $H^1_f(K_v, E[2]) = (\mathcal{O}_\mathfrak{q}^\times/\mathcal{O}_\mathfrak{q}^{\times 2})^2$.*
2. *If $\mathfrak{q}$ divides all the $c_i - c_j$ to the same even power, then $H^1_f(K_v, E[2])$ is the image of the 2-torsion, i.e. the three triples (2.1) and $(1,1,1)$.*

Let $m^{(i)} = (m_1^{(i)}, m_2^{(i)}, m_3^{(i)}) \in \mathrm{Sel}_2(E^i/K)$ be an element of the 2-Selmer group, for $i = 1, \ldots, n$. Let $\mathcal{M}$ be the set of triples $(m_1, m_2, m_3) \in (K^\times/K^{\times 2})^3$ with $m_1 m_2 m_3 = 1$, such that each m_j is in the subgroup generated by the elements $m_j^{(i)}$, $j = 1, 2, 3$ and $i = 1, \ldots, n$ in the group $K^\times/K^{\times 2}$.

Lemma 2.2.2. *[Skorobogatov and Swinnerton-Dyer, 2005, Lemma 9] Let E^i be elliptic curves with rational 2-torsion, for $i = 1, \ldots, n$.*

Let $m^{(i)} \in \mathrm{Sel}_2(E^i/K)$ be a fixed element of the 2-Selmer group of E^i for $i = 1, \ldots, n$. Suppose every element of $\mathcal{M}\backslash\{m^{(1)}, \ldots, m^{(n)}, (1,1,1)\}$ (defined above) is not everywhere locally solvable when viewed as 2-coverings of E^i for $i = 1, \ldots, n$. Then there exists a $b \in K^\times$ such that b is a unit and an integral square at each place in $S \supseteq \cup S(E^i)$ and the restricted 2-Selmer groups of E^i_b consists of just the identity element and the chosen element $m^{(i)}$, for $i = 1, \ldots, n$. Note: b is a square at the above places, but its prime factors may not be squares at these places. Furthermore, if $K = \mathbb{Q}$, then we may choose $b \equiv 1 \mod 8$. Again, the prime factors of b may not be squares at 2.

Furthermore, there also exists a $b \in K^\times$ such that the restricted 2-Selmer group of E^i_b consists of just the identity element, for $i = 1, \ldots, n$.

Proof. The first part of this statement is proved in Lemma 9 of [Skorobogatov and Swinnerton-Dyer, 2005], following the proof we see that the b is chosen so that b is a square unit at each of the bad places of the elliptic curve, extending this we get $b \in K_v^{\times 2}$ for $v \in S$. We provide an outline of the proof below.

Let $m = (m_1, m_2, m_3)$ be a triple which is a unit outside of S, and is not in $\mathcal{M}$. Let $\mathfrak{p}$ be a prime that is split in $L = K(\sqrt{m_1^{(i)}}, \sqrt{m_2^{(i)}}, \sqrt{m_3^{(i)}}, i = 1, \ldots, n)$ but does not split completely in $L(\sqrt{m_1}, \sqrt{m_2}, \sqrt{m_3})$, i.e. $m_j^{(i)} \in K_\mathfrak{p}^{\times 2}$ and at least one of m_1, m_2, m_3 is not in $K_\mathfrak{p}^{\times 2}$. Choose another prime $\mathfrak{p}'$ not in $S \cup \{\mathfrak{p}\}$ such that $\mathfrak{p}\mathfrak{p}' = (x)$ for some $x \in K^\times$ which is in $K_v^{\times 2}$ for all $v \in S$. The Hilbert product formula applied to $(m_j^{(i)}, x)$ shows that each $m_j^{(i)}$ is a square at $\mathfrak{p}'$.

Now choose a $\mathfrak{p}, \mathfrak{p}', x$ for each triple as above, where all the $\mathfrak{p}, \mathfrak{p}', x$ are distinct and let $b = \prod x$.

The 2-covering corresponding to $m^{(i)}$ for E_b^i is still locally solvable for $v \in S$, because b is locally a square there, and since $m_j^{(i)}$ is a square at each $\mathfrak{p}, \mathfrak{p}'$ implies that $m^{(i)}$ is locally solvable for E_b^i.

The 2-covering corresponding to m for E_b^i is not locally solvable at $\mathfrak{p}$ because some m_j is not locally a square at $\mathfrak{p}$ and each m_j is a unit at $\mathfrak{p}$. Hence the restricted 2-Selmer group of E_b^i is contained in $\mathcal{M}$. By the assumption above, if $m \in \mathcal{M} \backslash \{m^{(1)}, \ldots, m^{(n)}, (1,1,1)\}$ then it is not solvable at some place $w \in S$ as a 2-covering of E. Since $b \in {K_w^\times}^2$, the 2-covering m for E_b over K_w is isomorphic to the 2-covering m for E_b over K_w, and thus m is not solvable as a 2-covering for E_b. Thus the restricted 2-Selmer group of E_b consists of just $m^{(i)}$ and $(1,1,1)$.

The second part:

For each $\mathfrak{q} \in S$ use Chebotarev's density theorem to choose a prime $\mathfrak{p} = (p)$ of K, not in S and not dividing 3, such that $\left(\frac{p}{\mathfrak{q}}\right) = -1$ and $p \in {K_v^\times}^2$ for all $v \in S \setminus \{\mathfrak{q}\}$. At an archimedean place choose a prime, $\mathfrak{p} = (p)$, such that $\left(\frac{-1}{\mathfrak{p}}\right) = -1$ and $p \in {K_v^\times}^2$ for all $v \in S \setminus \{\mathfrak{q}\}$.

Now choose a $\mathfrak{p}$ for each $\mathfrak{q} \in S$, where all the $\mathfrak{p}$ are different and let $b = \prod p$. We want to show that the restricted 2-Selmer group of E_b^i is trivial, $i = 1, \ldots, n$.

Claim 2.2.3. *Suppose the triple $m = (m_1, m_2, m_3)$ is in the restricted 2-Selmer group of E_b^i and has odd valuation at $\mathfrak{q} \in S(E^i)$ then m is not locally soluble at $\mathfrak{p}$.*

Proof. We analyze the 2-Selmer group of E_b^i. By [Skorobogatov and Swinnerton-Dyer, 2005, Lemma 4 (25)] the image of the local Kummer map at the prime $\mathfrak{p}$ is given by $(1,1,1)$ and the image of the three 2-torsion triples. The restriction of m is not one of the latter three since, at $\mathfrak{p}$, the m_i are integral units (because m is in the restricted 2-Selmer group) and the image of the 2-torsion is divisible by $\mathfrak{p}$. Furthermore it is not $(1,1,1)$: w.l.o.g. assume $\mathrm{val}_\mathfrak{q}(m_1) > 0$ then $(m_1, p)_\mathfrak{p} = (m_1, p)_\mathfrak{q} = \left(\frac{p}{\mathfrak{q}}\right) = -1$, hence m_1 is not a square at $\mathfrak{p}$. □

Since S includes the archimedean places this shows that the restricted 2-Selmer group is trivial.

□

Remark 2.2.4. In the previous lemma we are trying to find a quadratic twist which removes all the elements of the original 2-Selmer groups of both E^i (except the chosen elements). This may introduce new element in $\mathrm{Sel}_2(E_b^i)$, but we know that these new elements are each divisible by a prime outside S.

Lemma 2.2.5. *Let E be the elliptic curve $y^2 = x^3 - n^2x$ over $\mathbb{Q}$ with $n \equiv 5 \mod 8$ a positive square-free integer such that at least one of its prime factors is $7 \mod 8$. Then in Lemma 2.2.2 above, b can be chosen such that each prime factor of b is congruent to 1 modulo 8.*

Proof. We simply need to show that any element of the Selmer group is divisible by some prime other than 2. Since the local condition at the prime 2 is given in Lemma 3.2.2. The only element that could restrict to a non-trivial element at the prime 2 and the trivial element at all the other primes is $(-1, -1, 1)$ and this element is not possible since there is a prime that is $7 \mod 8$, thus this element would not satisfy the correct local condition there. □

Lemma 2.2.6. *Let E be an elliptic curve with rational 2-torsion. Let E_b be a quadratic twist with a k-dimensional restricted 2-Selmer group ($k = 1$) coming from Lemma 2.2.2.*

1. *If $\dim \mathrm{Sel}_2(E_b/K) > 3 + k$, then there are two primes $\mathfrak{q}_0, \mathfrak{q}_1 | b$, such that $\mathrm{loc}_{\mathfrak{q}_0} \oplus \mathrm{loc}_{\mathfrak{q}_1}$ is at least 3-dimensional and sometimes surjective.*

2. *If $\dim \mathrm{Sel}_2(E_b/K) > 2 + k$ and $\mathfrak{q}_1$ is a chosen place of bad reduction, then there exists a $\mathfrak{q}_0 | b$ such that the image of the 2-Selmer group under the map $\mathrm{loc}_{\mathfrak{q}_0} \oplus \mathrm{loc}_{\mathfrak{q}_1}$ is at least 3-dimensional.*

Proof. Let $\mathfrak{q}_i$ denote the primes dividing b, which are principal by Lemma 2.2.2. Let $V_{\mathfrak{q}}$ denote the local condition at the prime $\mathfrak{q}$ for E. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_N$ be the primes dividing b. Let $u \in \mathrm{Sel}_2(E_b/K)$ lie in the complement of the vector space spanned by the restricted 2-Selmer group and the image of the 2-torsion and let $v \in \mathrm{Sel}_2(E_b/K)$ lie in the complement of the vector space spanned by the restricted 2-Selmer group, the image of the 2-torsion and u.

Then the image of the 2-torsion, u and v together span a 4-dimensional space in $\mathrm{Sel}_2(E_b/K)$, but in fact they span a 4-dimensional space in $V := \oplus_{i=1}^{N} V_{\mathfrak{q}_i}$ - if it didn't then a liner combination of those vectors would be in the span of the restricted 2-Selmer group and the image of the 2-torsion and thus u or v would be in that span, a contradiction. It is possible for this 4-dimensional space not to span $V_{\mathfrak{q}_0} \oplus V_{\mathfrak{q}_1}$ for some $\mathfrak{q}_0, \mathfrak{q}_1$. Since the image of the 2-torsion is a diagonal embedding in V it is likely that the 4-dimensional space does actually span $V_{\mathfrak{q}_0} \oplus V_{\mathfrak{q}_1}$ for some $\mathfrak{q}_0, \mathfrak{q}_1$, but this is not true in general.

For the second part: Let $v_1 \in \mathrm{Sel}_2(E_b/K)$ lie in the complement of the vector space spanned by the restricted 2-Selmer group and the image of the 2-torsion. Suppose each component of v_1 is a

unit at $\mathfrak{q}_1$, then there exists a $\mathfrak{q}_0$ such that v_1 has components with odd valuation at $\mathfrak{q}_0|b$ (because it is not in the restricted 2-Selmer group). Multiply v_1 by a triple from (2.1) to remove $\mathfrak{q}_0$. This product has components which are units at $\mathfrak{q}_0$ and has odd valuation at $\mathfrak{q}_1$ (since the torsion triples have odd valuation at $\mathfrak{q}_1$). Suppose v_1 is divisible by $\mathfrak{q}_1$ and without loss of generality suppose $\mathrm{loc}_{\mathfrak{q}_1}(v_1) = \mathrm{loc}_{\mathfrak{q}_1}(\mathrm{torsion}_1)$ where $\mathrm{torsion}_1$ is the first torsion triple in (2.1), then either there exists a $\mathfrak{q}_0|b$ such that v_1 is a unit at $\mathfrak{q}_0$ or v_1 is divisible by all $\mathfrak{q}_i|b$ and there exists a $\mathfrak{q}_0$ such that $\mathrm{loc}_{\mathfrak{q}_0}(v_1) \neq \mathrm{loc}_{\mathfrak{q}_0}(\mathrm{torsion}_1)$ (because otherwise v_1 times $\mathrm{torsion}_1$ is in the restricted 2-Selmer group, a contradiction). Multiply v_1 by a triple from (2.1) to remove $\mathfrak{q}_0$. This product has components which are units at $\mathfrak{q}_0$ and still has odd valuation at $\mathfrak{q}_1$ (since the localization at $\mathfrak{q}_0$ is not the image of $\mathrm{torsion}_1$). We refer to the final element in each case as v_1.

For a multiplicative place $\mathfrak{q}_1$: Let $v_1 \in \mathrm{Sel}_2(E_b/K)$ lie in the complement of the vector space spanned by the restricted 2-Selmer group and the image of the 2-torsion. Suppose some component of v_1 is divisible by $\mathfrak{q}_1$, then there is some $\mathfrak{q}_0|b$ such that $\mathrm{loc}_{\mathfrak{q}_0} \oplus \mathrm{loc}_{\mathfrak{q}_1}$ is at least 3-dimensional: If v_1 is not divisible by some $\mathfrak{q}_0$ then use that $\mathfrak{q}_0$. If v_1 is divisible by every $\mathfrak{q}_0|b$ then, since $\mathfrak{q}_1$ is a multiplicative place it divides exactly two of the torsion elements, there is some $\mathfrak{q}_0|b$ which divides v_1 times one of these torsion elements - since that product is not in the restricted 2-Selmer group - use this $\mathfrak{q}_0$.

Suppose each component of v_1 is a unit at $\mathfrak{q}_1$, then it is divisible by some $\mathfrak{q}_0|b$ since it is not in the restricted 2-Selmer group, use this $\mathfrak{q}_0$.

□

The next proposition shows that twisting by a non-square at one additive place keeps the 2-Selmer rank the same. This additive place is not necessarily a ramified place of a previous twist.

Proposition 2.2.7. *Let E be an elliptic curve with rational 2-torsion. Let $\mathfrak{q}_0$ be an additive place for E. Suppose $\mathfrak{p} = (\pi)$ is a prime such that $\pi \in {K_v^\times}^2$ for $v \in S\backslash\{\mathfrak{q}_0\}$ with $S \supseteq S(E)$ and $\left(\frac{\pi}{\mathfrak{q}_0}\right) = -1$. Then $\dim \mathrm{Sel}_2(E/K) = \dim \mathrm{Sel}_2(E_\pi/K)$. Furthermore, the restricted 2-Selmer group does not change, if its elements are units at $\mathfrak{q}_0$.*

Proof. Let $F = K(\sqrt{\pi})$ and $T = \{\mathfrak{q}_0, \mathfrak{p}\}$. By Lemma 2.2.1 we conclude that $H^1_f(K_v, E[2]) \cap H^1_f(K_v, E^F[2]) = 0$, when $v = \mathfrak{q}_0$ or $\mathfrak{p}$. Therefore we have satisfied all the requirements of Proposi-

tion 2.1.1. The proposition says that

$$\mathrm{d}_2(E^F/K) = \mathrm{d}_2(E/K) - \dim V_T + \dim V_T^F.$$

With the restriction that

$$\dim V_T + \dim V_T^F \leq \sum_{v \in T} \dim H_f^1(K_v, E[2]) = 4. \tag{2.3}$$

We see that $\mathrm{loc}_{\mathfrak{q}_0} : \mathrm{Sel}_2(E/K) \twoheadrightarrow H_f^1(K_{\mathfrak{q}_0}, E[2])$ is surjective because of the image of the 2-torsion. Similarly, $\mathrm{loc}_{\mathfrak{p}} : \mathrm{Sel}_2(E^F/K) \twoheadrightarrow H_f^1(K_{\mathfrak{p}}, E^F[2])$ is surjective. Hence $\dim V_T \geq 2$ and $\dim V_T^F \geq 2$ and by (2.3) these are equalities. □

Proposition 2.2.8. *Suppose E_b is a twisted elliptic curve with $\mathfrak{q}_0 = (q_0)$ and $\mathfrak{q}_1 = (q_1)$ ramified places of the quadratic field $K(\sqrt{b})/K$, hence places of additive reduction for E_b. Suppose that the restricted 2-Selmer group of E_b has dimension k, $k = 1$, and $\dim \mathrm{Sel}_2(E_b/K) > 3 + k$. Let $S \supseteq S(E_b)$ be a finite set of places of K. There exists a $c \in K^\times$ such that the ideal (c) is not divisible by a prime in S, and $c \in {\mathcal{O}_{K_\mathfrak{q}}^\times}^2$ for $\mathfrak{q} \in S \setminus \{\mathfrak{q}_0, \mathfrak{q}_1\}$.*

1. *If $\mathrm{loc}_{\mathfrak{q}_0,\mathfrak{q}_1} : \mathrm{Sel}_2(E_b/K) \to H_f^1(K_{\mathfrak{q}_0}, E_b[2]) \oplus H_f^1(K_{\mathfrak{q}_1}, E_b[2])$ is surjective (e.g. if $\mathfrak{q}_0, \mathfrak{q}_1$ satisfy part 1 of Lemma 2.2.6), then*

$$\dim \mathrm{Sel}_2(E_c/K) = \dim \mathrm{Sel}_2(E_b/K) - 2.$$

2. *If the image of $\mathrm{Sel}_2(E_b/K)$ under $\mathrm{loc}_{\mathfrak{q}_0,\mathfrak{q}_1}$ has dimension three, then*

$$\dim \mathrm{Sel}_2(E_c/K) = \dim \mathrm{Sel}_2(E_b/K).$$

Furthermore the restricted 2-Selmer group does not change, if its elements are units at $\mathfrak{q}_1$.

Proof. Let $\mathfrak{p} = (\pi)$ be a prime ideal not in $S \supseteq S(E_b)$ such that $\left(\frac{\pi}{\mathfrak{q}_0}\right) = -1 = \left(\frac{\pi}{\mathfrak{q}_1}\right)$ and $\pi \in {\mathcal{O}_{K_\mathfrak{q}}^\times}^2$ for $\mathfrak{q} \in S \setminus \{\mathfrak{q}_0, \mathfrak{q}_1\}$. Let $c = b\pi$.

Let $F = K(\sqrt{\pi})$ and $T = \{\mathfrak{q}_0, \mathfrak{q}_1, \mathfrak{p}\}$. All places of S outside of T are split in F, so the local condition doesn't change there. By Lemma 2.2.1 we again conclude that $H_f^1(K_v, E_b[2]) \cap H_f^1(K_v, E_b^F[2]) = 0$, when $v = \mathfrak{q}_0, \mathfrak{q}_1$ or $\mathfrak{p}$. Therefore we have satisfied all the requirements of Proposition 2.1.1. Then the proposition says that

$$\mathrm{d}_2(E_b^F/K) = \mathrm{d}_2(E_b/K) - \dim V_T + \dim V_T^F.$$

With the restriction that

$$\dim V_T + \dim V_T^F \leq \dim \sum_{v \in T} H_f^1(K_v, E_b[2]) = 6. \tag{2.4}$$

We see that $\mathrm{loc}_{\mathfrak{q}_0} : \mathrm{Sel}_2(E_b/K) \twoheadrightarrow H_f^1(K_{\mathfrak{q}_0}, E_b[2])$ is surjective because of the image of the 2-torsion. Similarly, $\mathrm{loc}_{\mathfrak{p}} : \mathrm{Sel}_2(E_b^F/K) \twoheadrightarrow H_f^1(K_{\mathfrak{p}}, E_b^F[2])$ is surjective. Hence $\dim V_T \geq 2$. and $\dim V_T^F \geq 2$.

Then by Lemma 2.2.6, $\dim V_T$ is 4. Then by (2.4), $\dim V_T^F = 2$ as desired.

The second part follows from the above bounds and because $\dim V_T$ and $\dim V_T^F$ have the same parity, see Lemma 2.1.2. □

Proposition 2.2.9. *Let E be an elliptic curve with rational 2-torsion. Let $\mathfrak{q}_0 = (q_0)$ be an additive place for E. Suppose $\mathfrak{q}_0' = (q_0')$ is a prime such that $\left(\frac{q_0'}{v}\right) = \left(\frac{q_0}{v}\right)$ for $v \in S \backslash \{\mathfrak{q}_0\}$ with $S \supseteq S(E)$. Then $\dim \mathrm{Sel}_2(E/K) = \dim \mathrm{Sel}_2(E_{q_0 q_0'}/K)$. Furthermore, any element of the 2-Selmer group of E that is divisible by $\mathfrak{q}_0$ is an element of the 2-Selmer group of E^F once q_0 is replaced by q_0'.*

Proof. Let $F = K(\sqrt{q_0 q_0'})$ and $T = \{\mathfrak{q}_0, \mathfrak{q}_0'\}$. Since F/K is split outside of T the local conditions do not change there. By Lemma 2.2.1 we can explicitly describe $H_f^1(K_v, E[2])$, and it is particularly simple for places of good reduction and certain additive places. In particular we conclude that $H_f^1(K_v, E[2]) \cap H_f^1(K_v, E^F[2]) = 0$, when $v = \mathfrak{q}_0$ or $\mathfrak{q}_0'$. Therefore we have satisfied all the requirements of Proposition 2.1.1. The proposition says that

$$\mathrm{d}_2(E^F/K) = \mathrm{d}_2(E/K) - \dim V_T + \dim V_T^F.$$

With the restriction that

$$\dim V_T + \dim V_T^F \leq \sum_{v \in T} \dim H_f^1(K_v, E[2]) = 4. \tag{2.5}$$

We see that $\mathrm{loc}_{\mathfrak{q}_0}$ is surjective for E by because of the image of the 2-torsion. Also, $\mathrm{loc}_{\mathfrak{q}_0'}$ is surjective for E^F because of the image of the 2-torsion. Therefore we conclude that $\dim V_T^F \geq 2$ and $\dim V_T \geq 2$. Since this is the maximum that the sum can be the inequalities are equalities and hence $\mathrm{d}_2(E^F/K) = \mathrm{d}_2(E/K) = \mathrm{d}_2(E/K) - 2$, as desired.

□

Chapter 3

Elliptic curves with only good or additive reduction

Suppose our elliptic curves only have places of additive or good reduction. We would like to find a single twist that gives them both essential 2-Selmer rank one. If we applied Proposition 2.2.8 to finitely many elliptic curves then the 2-Selmer rank of each of the elliptic curves would be reduced by 2. We would like something more refined - where we can reduce the 2-Selmer rank of each elliptic curve while keeping the others the same.

For simplicity we first demonstrate the proposition for one elliptic curve and then for finitely many elliptic curves.

3.1 Reducing the 2-Selmer rank by 2

Proposition 3.1.1. *Let E/K be an elliptic curve and let $\mathfrak{q}_0, \mathfrak{q}_1$ be two primes of additive reduction for E. Let $S \supseteq S(E)$ be a finite set of places of K. Then there exists a $c \in K^\times$ such that $c \in {\mathcal{O}_{K_\mathfrak{q}}^\times}^2$ for $\mathfrak{q} \in S \setminus \{\mathfrak{q}_0, \mathfrak{q}_1\}$.*

If $\mathrm{loc}_{\mathfrak{q}_0,\mathfrak{q}_1} : \mathrm{Sel}_2(E/K) \to H^1_f(K_{\mathfrak{q}_0}, E[2]) \oplus H^1_f(K_{\mathfrak{q}_1}, E[2])$ is ...

- *4-dimensional then*

$$\dim \mathrm{Sel}_2(E_c/K) = \dim \mathrm{Sel}_2(E/K) - 2.$$

- *3-dimensional then*

$$\dim \mathrm{Sel}_2(E_c/K) = \dim \mathrm{Sel}_2(E/K).$$

- *2-dimensional then*

$$\dim \mathrm{Sel}_2(E_c/K) = \dim \mathrm{Sel}_2(E/K).$$

Proof. We first set some notation that will be used in the proof.

1. Let $\mathfrak{p} = (\pi)$ be a prime ideal not in S such that $\left(\frac{\pi}{\mathfrak{q}_0}\right) = -1 = \left(\frac{\pi}{\mathfrak{q}_1}\right)$ and $\pi \in {\mathcal{O}_{K_\mathfrak{q}}^\times}^2$ for $\mathfrak{q} \in S \setminus \{\mathfrak{q}_0, \mathfrak{q}_1\}$.

2. Let $\mathfrak{q}_0' = (q_0')$ be a prime ideal not in $S \cup S(E_\pi)$ such that $q_0' = \lambda q_0$ (modulo squares), and $\lambda \in {K_\mathfrak{q}^\times}^2$ for all $\mathfrak{q} \in S \backslash \{\mathfrak{q}_0\}$ and $\left(\frac{\lambda}{\mathfrak{p}}\right) = -1$. Let $\pi' \in K^\times$ be such that $\mathfrak{p}' = (\pi')$ is a prime ideal not in $S \cup S(E_{\pi q_0'})$, and $\pi' \in {K_\mathfrak{q}^\times}^2$ for all $\mathfrak{q} \in S$ and $\left(\frac{\pi'}{\mathfrak{p}}\right) = -1$ and $\left(\frac{\pi'}{\mathfrak{q}_0'}\right) = -1$.

Proof when the image of $\mathrm{loc}_{\mathfrak{q}_0,\mathfrak{q}_1}$ is 2-dimensional

We first analyze how the 2-Selmer rank changes after twisting by π. Let $F = K(\sqrt{\pi})$ and $T = \{\mathfrak{q}_0, \mathfrak{q}_1, \mathfrak{p}\}$. All places of S outside of T are split in F, so the local condition doesn't change there. By Lemma 2.2.1 we conclude that $H_f^1(K_v, E[2]) \cap H_f^1(K_v, E^F[2]) = 0$, when $v = \mathfrak{q}_0, \mathfrak{q}_1$ or $\mathfrak{p}$. Therefore we have satisfied all the requirements of Proposition 2.1.1. Then the proposition says that

$$\mathrm{d}_2(E^F/K) = \mathrm{d}_2(E/K) - \dim V_T + \dim V_T^F.$$

With the restriction that

$$\dim V_T + \dim V_T^F \leq \dim \sum_{v \in T} H_f^1(K_v, E[2]) = 6. \tag{3.1}$$

By assumption $\dim V_T = 2$. We see that $\mathrm{loc}_\mathfrak{p} : \mathrm{Sel}_2(E^F/K) \twoheadrightarrow H_f^1(K_\mathfrak{p}, E^F[2])$ is surjective because of the image of the 2-torsion, hence $\dim V_T^F \geq 2$. Then by (3.1) and Lemma 2.1.2, $\dim V_T^F$ is either 2 or 4.

If $\dim V_T^F = 2$ then $c = \pi$ satisfies the conditions of the proposition.

If V_T^F is not 2-dimensional then it must be 4-dimensional.

Since the image of the 2-torsion is surjective onto each 2-dimensional subspace, $H_f^1(K_v, E[2])$, we can translate both of the two 'new' vectors (not the image of the 2-torsion) to get vectors which fall into one of four types:

a) If it is trivial at $\mathfrak{p}$ and non-trivial at exactly one of $\mathfrak{q}_0$ or $\mathfrak{q}_1$ then it wouldn't satisfy the correct local condition at $\mathfrak{p}$, since it is not a square at $\mathfrak{p}$

b) If it is trivial at exactly one of $\mathfrak{q}_0, \mathfrak{q}_1$ and non-trivial at $\mathfrak{p}$ then it has the wrong condition at $\mathfrak{p}$, since the local condition there is $(1,1,1)$ and permutations of $(\pi,\pi,1)$.

c) If it is trivial at $\mathfrak{q}_0$ and $\mathfrak{q}_1$ and not at $\mathfrak{p}$, or equivalently it is trivial at $\mathfrak{p}$ and non-trivial at $\mathfrak{q}_0, \mathfrak{q}_1$. These are potentially non-trivial.

d) If it is non-trivial in all three components, then $\mathrm{loc}_{\mathfrak{q}_0}$ and $\mathrm{loc}_{\mathfrak{q}_1}$ must be the image of the same 2-torsion element, otherwise it does not satisfy the correct condition at $\mathfrak{p}$. Therefore, any such vector is the image of the 2-torsion.

Thus the only way $\dim V_T^F = 4$ is if we have two vectors of type c) above. Hence $\mathrm{loc}_{\mathfrak{p},\mathfrak{q}_0}$ is surjective for E_π.

Now we analyze how the 2-Selmer rank changes under the remaining quadratic twists.

Let $F' = K(\sqrt{q_0 q_0' \pi'})$ and $T' = \{\mathfrak{q}_0, \mathfrak{q}_0', \mathfrak{p}'\}$ and for simplicity let $E' = E_\pi$. Since F'/K is split outside of T' the local conditions do not change there. By Lemma 2.2.1 we can explicitly describe $H_f^1(K_v, E'[2])$, and it is particularly simple for places of good reduction and certain additive places. In particular we conclude that $H_f^1(K_v, E'[2]) \cap H_f^1(K_v, E'^{F'}[2]) = 0$, when $v = \mathfrak{q}_0, \mathfrak{q}_0'$ or $\mathfrak{p}'$. Therefore we have satisfied all the requirements of Proposition 2.1.1. The proposition says that

$$\mathrm{d}_2(E'^{F'}/K) = \mathrm{d}_2(E'/K) - \dim V_{T'} + \dim V_{T'}^{F'}.$$

With the restriction that

$$\dim V_{T'} + \dim V_{T'}^{F'} \leq \sum_{v \in T'} \dim H_f^1(K_v, E'[2]) = 6. \tag{3.2}$$

Since $\mathrm{loc}_{\mathfrak{p},\mathfrak{q}_0}$ is surjective for E', $\dim V_{T'} \geq 4$. Also, $\mathrm{loc}_v : \mathrm{Sel}_2(E'^{F'}/K) \twoheadrightarrow H_f^1(K_v, E'^{F'}[2])$ is surjective for $v = \mathfrak{q}_0', \mathfrak{p}'$ because of the image of the 2-torsion, thus $\dim V_{T'}^{F'} \geq 2$. Since this is the maximum that the sum can be by (3.2) the inequalities are equalities and hence $\mathrm{d}_2(E'^{F'}/K) = \mathrm{d}_2(E'/K) - 2 = \mathrm{d}_2(E/K)$.

In this situation (i.e. if $\dim V_T^F = 4$) let $c = \pi\pi'\lambda = \pi\pi' q_0 q_0'$. Therefore $\mathrm{d}_2(E_c/K) = \mathrm{d}_2(E/K)$.

Proof when the image of $\mathrm{loc}_{\mathfrak{q}_0,\mathfrak{q}_1}$ is 3-dimensional

We first analyze how the 2-Selmer rank changes after twisting by π. By Proposition 2.2.8 part 2, we see that the 2-Selmer rank does not change. Therefore, $c = \pi$ satisfies the conditions of the

proposition. Furthermore, by the analysis in the proof of the 2-dimensional case we know that the 2-Selmer group of E_π contains an element that is divisible by π and not divisible by q_0, q_1, call this element u.

Now we analyze how the 2-Selmer rank changes under the remaining quadratic twists. Let $F' = K(\sqrt{q_0 q_0' \pi'})$ and $T' = \{\mathfrak{q}_0, \mathfrak{q}_0', \mathfrak{p}'\}$ as in the previous case. Thus,

$$\dim V_{T'} + \dim V_{T'}^{F'} \leq \sum_{v \in T'} \dim H_f^1(K_v, E'[2]) = 6. \tag{3.3}$$

We see that $\mathrm{loc}_{\mathfrak{p},\mathfrak{q}_0}$ is 3-dimensional for $E' = E_\pi$ because of the image of the 2-torsion and the element u, above. Also, $\mathrm{loc}_v : \mathrm{Sel}_2(E'^{F'}/K) \twoheadrightarrow H_f^1(K_v, E'^{F'}[2])$ is surjective for $v = \mathfrak{q}_0', \mathfrak{p}'$ because of the image of the 2-torsion. By Lemma 2.1.2, we must have $\dim V_{T'}^{F'} \equiv \dim V_{T'} \mod 2$. Therefore $\dim V_{T'}^{F'} = 3$ and $\dim V_{T'} = 3$, since this is the maximum that the sum can be. Let $c = \pi\pi'\lambda = \pi\pi' q_0 q_0'$, then since $\mathrm{d}_2(E_c/K) = \mathrm{d}_2(E/K)$, this value of c also satisfies the conditions of the proposition.

Proof when the image of $\mathrm{loc}_{\mathfrak{q}_0,\mathfrak{q}_1}$ is 4-dimensional

We first analyze how the 2-Selmer rank changes when $c = \pi$. Let $F = K(\sqrt{\pi})$ and $T = \{\mathfrak{q}_0, \mathfrak{q}_1, \mathfrak{p}\}$. All places of S outside of T are split in F, so the local condition doesn't change there. By Lemma 2.2.1 we conclude that $H_f^1(K_v, E[2]) \cap H_f^1(K_v, E^F[2]) = 0$, when $v = \mathfrak{q}_0, \mathfrak{q}_1$ or $\mathfrak{p}$. Therefore we have satisfied all the requirements of Proposition 2.1.1. Then the proposition says that

$$\mathrm{d}_2(E^F/K) = \mathrm{d}_2(E/K) - \dim V_T + \dim V_T^F.$$

With the restriction that

$$\dim V_T + \dim V_T^F \leq \dim \sum_{v \in T} H_f^1(K_v, E[2]) = 6. \tag{3.4}$$

By assumption $\dim V_T = 4$. We see that $\mathrm{loc}_{\mathfrak{p}} : \mathrm{Sel}_2(E^F/K) \twoheadrightarrow H_f^1(K_{\mathfrak{p}}, E^F[2])$ is surjective because of the image of the 2-torsion, hence $\dim V_T^F \geq 2$. By (3.4) we conclude that $\dim V_T^F = 2$ and thus $\mathrm{d}_2(E_c/K) = \mathrm{d}_2(E/K) - 2$ and $c = \pi$ suffices.

Next we analyze how the 2-Selmer rank changes when $c = \pi\pi'\lambda = \pi\pi' q_0 q_0'$.

Since $\mathrm{loc}_{\mathfrak{q}_0,\mathfrak{q}_1}$ is 4 dimensional, we can choose two elements $u, v \in \mathrm{Sel}_2(E/K)$ such that u is divisible by q_1 but not divisible by q_0 and v is divisible by q_0 but not divisible by q_1. We rearrange the quadratic twists so that we first twist by $q_0 q_0'$, by Proposition 2.2.9 the 2-Selmer rank does not

change. Furthermore, u, v will change to two elements (which we continue to call u, v) such that u is divisible by q_1 but not divisible by q_0', q_0 and v is divisible by q_0' but not divisible by q_1, q_0.

Next we twist by π, which is not a square at $\mathfrak{q}_1$ and is a square at all other primes in $S(E_{q_0 q_0'})$. Thus by Proposition 2.2.7 the 2-Selmer rank of $E_{q_0 q_0' \pi}$ is the same as the 2-Selmer rank of $E_{q_0 q_0'}$. Furthermore, u, v will change to two elements (which we continue to call u, v) such that u is divisible by q_1, π but not divisible by q_0', q_0 and v is divisible by q_0' but not divisible by q_1, q_0, π.

Next we analyze the quadratic twist by π', for simplicity let $E'' = E_{q_0 q_0' \pi}$. Let $F'' = K(\sqrt{\pi'})$ and $T'' = \{\mathfrak{q}_0', \mathfrak{p}, \mathfrak{p}'\}$. Since F''/K is split outside of T'' the local conditions do not change there. By Lemma 2.2.1 we can explicitly describe $H^1_f(K_v, E''[2])$, and it is particularly simple for places of good reduction and certain additive places. In particular we conclude that $H^1_f(K_v, E''[2]) \cap H^1_f(K_v, E''^{F''}[2]) = 0$, when $v = \mathfrak{q}_0', \mathfrak{p}$ or $\mathfrak{p}'$. Therefore we have satisfied all the requirements of Proposition 2.1.1. The proposition says that

$$\mathrm{d}_2(E''^{F''}/K) = \mathrm{d}_2(E''/K) - \dim V_{T''} + \dim V_{T''}^{F''}.$$

With the restriction that

$$\dim V_{T''} + \dim V_{T''}^{F''} \leq \sum_{v \in T''} \dim H^1_f(K_v, E''[2]) = 6. \tag{3.5}$$

We see that $\mathrm{loc}_{\mathfrak{p}, \mathfrak{q}_0'}$ is surjective for E'' because of u, v above. Also, $\mathrm{loc}_v : \mathrm{Sel}_2(E''^{F''}/K) \twoheadrightarrow H^1_f(K_v, E''^{F''}[2])$ is surjective for $v = \mathfrak{q}_0', \mathfrak{p}'$ because of the image of the 2-torsion. Therefore we conclude that $\dim V_{T''}^{F''} \geq 2$ and $\dim V_{T''} \geq 4$. Since this is the maximum that the sum can be, the inequalities are equalities and hence $\mathrm{d}_2(E''^{F''}/K) = \mathrm{d}_2(E''/K) - 2 = \mathrm{d}_2(E/K) - 2$, as desired. Let $c = \pi \pi' \lambda = \pi \pi' q_0 q_0'$, then this value of c also satisfies the conditions of the proposition.

□

3.2 Reducing the 2-Selmer rank for $y^2 = x^3 - n^2 x$

In this section we only consider the congruent number elliptic curves, $y^2 = x^3 - n^2 x$ over $\mathbb{Q}$ with n a positive square-free integer..

Proposition 3.2.1. *Let E be the elliptic curve $y^2 = x^3 - n^2 x$ over $\mathbb{Q}$ with n a positive square-free integer. Then $d_2(E/\mathbb{Q})$ is even if $n \equiv 1, 2, 3 \mod 8$ and odd if $n \equiv 5, 6, 7 \mod 8$.*

Proof. This is a theorem due to Birch-Stephens and is clearly stated in [Heath-Brown, 1994, Theorem in the Appendix]. □

Lemma 3.2.2. *Let E be the elliptic curve $y^2 = x^3 - n^2x$ over $\mathbb{Q}$ with $n \equiv 1, 7 \mod 8$ a positive square-free integer such that all of its prime factors are $1, 7 \mod 8$. Then the image of the local condition at the prime 2 is 2-dimensional.*

In particular, when applying Proposition 2.1.1 for the elliptic curves given above, the dimension of the local condition at the prime 2 can be taken to be 2-dimensional.

Proof. In general the local condition at the prime 2 is 3-dimensional and is given by the image of the 2-torsion and one additional element. As elements in $(\mathbb{Q}^\times/\mathbb{Q}^\times)^3$ the image of the 2-torsion, for the congruent number elliptic curve above, is given by: $(1,1,1), (-1,-n,n), (n,2,2n), (-n,-2n,2)$. The third element of the basis depends on the class of n modulo 8 and is given by:

$$\begin{cases} (-1,3,-3) & n \equiv 1 \mod 8 \\ (-1,1,-1) & n \equiv 3 \mod 8 \\ (-1,-1,1) & n \equiv 5 \mod 8 \\ (-1,-3,3) & n \equiv 7 \mod 8. \end{cases}$$

Thus if $n \equiv 1, 7 \mod 8$ and all of its prime factors are $\pm 1 \mod 8$ then it is not possible to map to the third element of given above. This is sufficient since the image of the 2-torsion maps to a 2-dimensional subspace of the local condition and excluding any element shows that it cannot be 3-dimensional.

The last part of the proposition follows from the fact that the image of the local condition at the prime 2 will always be 2-dimensional. □

Lemma 3.2.3. *Let E be the elliptic curve $y^2 = x^3 - n^2x$ over $\mathbb{Q}$ with $n \equiv 7 \mod 8$ a positive square-free integer such that all but one of its prime factors are $1 \mod 8$ and one is $7 \mod 8$. Let E_b be a quadratic twist with a k-dimensional restricted 2-Selmer group ($k = 1$) coming from Lemma 2.2.2.*

If $\dim \mathrm{Sel}_2(E_b/K) > 3+k$, then there are two primes $\mathfrak{q}_0, \mathfrak{q}_1 | b$, such that $\mathrm{loc}_{\mathfrak{q}_0} \oplus \mathrm{loc}_{\mathfrak{q}_1}$ is surjective.

Proof. Let $\mathfrak{q}_0, \ldots, \mathfrak{q}_N$ be the primes dividing b.

Outline: Let $u \in \mathrm{Sel}_2(E_b/K)$ lie in the complement of the vector space spanned by the restricted 2-Selmer group and the image of the 2-torsion and we choose u such that it is not divisible by the prime which is 7 mod 8 and maps to one of the first two elements of the local condition at the prime 2, see Lemma 3.2.2 - this is possible by adding an element of the 2-torsion. Then since these elements are symmetric (two of the components are the same), and by [Skorobogatov and Swinnerton-Dyer, 2005, Lemma 4] the local condition at all the odd places which are 1 mod 8, is completely symmetric (any permutation of a triple is another triple satisfying the local condition) we can swap two of the components of u to get another element of the 2-Selmer group, and these two elements (along with the image of the 2-torsion) will span a 4-dimensional subspace, i.e. $\mathrm{loc}_{\mathfrak{q}_0} \oplus \mathrm{loc}_{\mathfrak{q}_1}$ is surjective.

Let q_N be the prime which is 7 mod 8. Let $v', w' \in \mathrm{Sel}_2(E_b/K)$ lie in the complement of the vector space spanned by the restricted 2-Selmer group and the image of the 2-torsion. After shifting by one of the 2-torsion elements, v' can be shifted to an element which is not divisible by q_N, denote this element by v. Similarly define w from w'.

Of the elements $v, w, v+w$, at least one of the three is a vector such that $\mathrm{loc}_2(v) \in \{(1,1,1),(-1,1,-1),(1,2,2)\}$, denote this vector, $v = (v_1, v_2, v_3)$. There exist two primes $\mathfrak{q}_0, \mathfrak{q}_1 | b$, such that $\mathrm{loc}_{\mathfrak{q}_0} \oplus \mathrm{loc}_{\mathfrak{q}_1}$ is 3-dimensional, since this vector is not in the restricted 2-Selmer group.

Now we find the last element, to make this map surjective. Without loss of generality suppose $\mathrm{loc}_2(v) = (-1,1,-1)$, then let $w = (v_3, v_2, v_1)$. This element has the correct localization at the prime 2, and by [Skorobogatov and Swinnerton-Dyer, 2005, Lemma 4] the local condition at all the odd places is completely symmetric (any permutation of a triple is another triple satisfying the local condition), thus w is another element of the 2-Selmer group, and these two elements (along with the image of the 2-torsion) will span a 4-dimensional subspace, i.e. $\mathrm{loc}_{\mathfrak{q}_0} \oplus \mathrm{loc}_{\mathfrak{q}_1}$ is surjective.

□

Lemma 3.2.4. *Let E be the elliptic curve $y^2 = x^3 - n^2 x$ over $\mathbb{Q}$ with either,*

- *$n \equiv 5$ mod 8 a positive square-free integer such that all but one of its prime factors are ± 1 mod 8 and one is 5 mod 8.*
- *$n \equiv 7$ mod 8 a positive square-free integer such that all but one of its prime factors are ± 3 mod 8 and one is 7 mod 8.*

Let E_b be a quadratic twist with a k-dimensional restricted 2-Selmer group ($k = 1$) coming from Lemma 2.2.2.

If $\dim \mathrm{Sel}_2(E_b/K) > 3+k$, *then there are two primes* $\mathfrak{q}_0, \mathfrak{q}_1 | b$, *such that* $\mathrm{loc}_{\mathfrak{q}_0} \oplus \mathrm{loc}_{\mathfrak{q}_1}$ *is surjective.*

Proof. Let $\mathfrak{q}_0, \ldots, \mathfrak{q}_N$ be the primes dividing b. First part:

Let q_N be the prime which is 5 mod 8. Let $v', w' \in \mathrm{Sel}_2(E_b/K)$ lie in the complement of the vector space spanned by the restricted 2-Selmer group and the image of the 2-torsion. After shifting by one of the 2-torsion elements, v' can be shifted to an element which is not divisible by q_N, denote this element by v. Similarly define w from w'.

By Lemma 3.2.2 we can describe the local condition at the prime 2 for E. There are only two possibilities for the local condition at 2 of $v, w, v+w$ since they are not divisible by any prime that is 5 mod 8. The two possibilities are $(1,1,1), (-1,-1,1)$.

Of the elements $v, w, v+w$, at least one of the three is a vector such that $\mathrm{loc}_2(v) = (1,1,1)$, denote this vector, $v = (v_1, v_2, v_3)$. There exist two primes $\mathfrak{q}_0, \mathfrak{q}_1 | b$, such that $\mathrm{loc}_{\mathfrak{q}_0} \oplus \mathrm{loc}_{\mathfrak{q}_1}$ is 3-dimensional, since this vector is not in the restricted 2-Selmer group.

Now we find the last element, to make this map surjective. Let $w = (v_3, v_2, v_1)$. This element has the correct localization at the prime 2, and by [Skorobogatov and Swinnerton-Dyer, 2005, Lemma 4] the local condition at all the odd places is completely symmetric (any permutation of a triple is another triple satisfying the local condition), thus w is another element of the 2-Selmer group, and these two elements (along with the image of the 2-torsion) will span a 4-dimensional subspace, i.e. $\mathrm{loc}_{\mathfrak{q}_0} \oplus \mathrm{loc}_{\mathfrak{q}_1}$ is surjective.

Second part:

The proof is almost identical to the previous case. Let q_N be the prime which is 7 mod 8 and let v, w be as above. There are only three possibilities for the local condition at 2 of $v, w, v+w$ since they are not divisible by any prime that is 7 mod 8. The three possibilities are $(1,1,1), (1,2,2), (1,5,5)$.

With the three elements $v, w, v+w$, at least one of the three is a vector such that its image at 2 is $(1,1,1)$ - suppose otherwise then the three vectors map to the other two possibilities, and then at least one of the two possibilities has two vectors mapping to it, then their sum maps to $(1,1,1)$. Denote this vector, $v = (v_1, v_2, v_3)$, then the rest of the proof proceeds as above. □

Theorem 3.2.5. *Let $E^1, E^2/\mathbb{Q}$ be elliptic curves of the form $y^2 = x^3 - n_i^2 x$ over $\mathbb{Q}$ with n_i a*

positive square-free integer such that

- $n_i \equiv 5 \mod 8$ *a positive square-free integer such that all but one of its prime factors are* $\pm 1 \mod 8$ *and one is* $5 \mod 8$.
- $n_i \equiv 7 \mod 8$ *a positive square-free integer such that all but one of its prime factors are* $\pm 3 \mod 8$ *and one is* $7 \mod 8$.

Let $\mathfrak{q}_1, \tilde{\mathfrak{q}_1} \equiv 1 \mod 8$ *be distinct places of additive reduction for* E^1, E^2*, respectively. Furthermore, let* $b \in \mathbb{Z}$ *be such that* E^1_b, E^2_b *have* 1*-dimensional restricted 2-Selmer group (e.g. see Lemma 2.2.2). Assume that the essential 2-Selmer rank of* E^1_b *is at least two. Then there exist infinitely many* $c \in \mathbb{Z}$ *such that,*

1. $\dim \mathrm{Sel}_2(E^1_{bc}) = \dim \mathrm{Sel}_2(E^1_b) - 2 \quad \dim \mathrm{Sel}_2(E^2_{bc}) \leq \dim \mathrm{Sel}_2(E^2_b)$.
2. *Furthermore,* $c \in \mathbb{Z}_v^\times$ *for* $v \in \cup S(E^i)$ *and* -1 *is not a square at* c*. (In particular,* $c \equiv 1 \mod 8$*.)*
3. *The elements of the restricted 2-Selmer group of* E^i_b *which are units at* $\mathfrak{q}_1$ *are also in the restricted 2-Selmer group of* E^i_{bc}*.*
4. *If the 2-Selmer rank of* E^i_b *is odd, for* $i = 1, 2$*. Then there exist infinitely many* $c \in \mathbb{Z}$ *such that the quadratic twists* E^i_c *each have essential 2-Selmer rank* 1*.*

Proof. By assumption the 2-Selmer group of E^1_b has essential 2-Selmer rank at least 2, thus by Lemma 3.2.4, we get two primes $\mathfrak{q}_0, \mathfrak{q}_1 | b$ such that $\mathrm{loc}_{\mathfrak{q}_0,\mathfrak{q}_1}$ is 4-dimensional. Now apply Proposition 3.1.1, where $S = \cup S(E^i_b)$, this give a c satisfying the correct condition for E^1.

The 2-Selmer rank of E^2_{bc} is less than or equal to the 2-Selmer rank of E^2_{bc}, since by Proposition 3.1.1 the 2-Selmer rank will not increase.

Furthermore, $c \in {\mathbb{Z}_v^\times}^2$ for $v \in \cup S(E^i) \setminus \{\mathfrak{q}_0, \mathfrak{q}_1\}$ since this is the case for Proposition 3.1.1. Since $\mathfrak{q}_0 | b$ the quadratic twist does not effect the elements of the restricted 2-Selmer group which are units at $\mathfrak{q}_1$. Thus the restricted 2-Selmer group of E^i_b is a subgroup of $\mathrm{Sel}_2(E^i_{bc}/\mathbb{Q})$.

The last statement follows by applying the first one repeatedly (this is possible by the second property) and changing the roles of E^1 and the E^2 as necessary. □

3.3 More generally

By Proposition 3.1.1 we can reduce the 2-Selmer rank, but there is no procedure above to change the parity of the 2-Selmer rank. It is shown in Theorem 1 of [Dokchitser and Dokchitser, 2009] that the quadratic twists of an elliptic curve have constant 2-Selmer rank parity if and only if K has no real places and E has good reduction in some *abelian* extension. Furthermore, in [Connell, 1993] Proposition 1 and Proposition 6, Connell shows which elliptic curves have semistable reduction over an abelian extension. Over $\mathbb{Q}$ the description is explicitly given in terms of properties of the j-invariant. Over a number field, a similar description is given, except it excludes $j = 0, 1728$ and is somewhat less explicit.

We would like to consider twists that do not involve a real place, since those twists change the parity of both elliptic curves and not just one of them.

Lemma 3.3.1. *In this lemma we exclude twists which are not totally positive.*

- *If an elliptic curve only has places of additive or good reduction over $\mathbb{Q}$ then it has constant 2-Selmer parity if and only if its j-invariant appears on the list in [Connell, 1993, Proposition 1].*
- *If an elliptic curve only has places of additive or good reduction over a number field and $j \neq 0, 1728$ then it has constant 2-Selmer parity if and only if its j-invariant appears on the list in [Connell, 1993, Proposition 6].*

Proof. This follows from [Dokchitser and Dokchitser, 2009, Theorem 1], [Connell, 1993, Propositions 1 and 6] and the fact that multiplicative reduction only lifts to multiplicative reduction under extension of the base field. □

Therefore if the j-invariants of our elliptic curves are not on the lists referenced above then we can change their 2-Selmer parity and get a procedure similar to the one in Chapter 1. By Lemma 2.1.2 this will require twisting by a prime that is not a square at 2 and/or 3. We demonstrate such a procedure by describing it for the congruent number elliptic curve, $y^2 = x^3 - n^2x$.

A result of Kobayashi, [Kobayashi, 2002, Theorem 1.1], shows that over number fields this elliptic curve and any quadratic twist will have the same root number at 3. Which combined with Lemma 2.1.2 shows that we should look at the prime 2. See for example

Then using Proposition 3.2.1 we get the following.

Corollary 3.3.2. *Let E be the elliptic curve $y^2 = x^3 - n^2x$ over $\mathbb{Q}$. Suppose $\pi \in \mathbb{Q}^\times$ such that $\mathfrak{p} = (\pi)$ is a prime ideal not in $S(E)$ and $\pi \in {\mathbb{Q}_v^\times}^2$ for all $v \in S\backslash\{2\}$.*

If $2 \nmid n$ then $$d_2(E_\pi/\mathbb{Q}) \begin{cases} \not\equiv d_2(E/\mathbb{Q}) \mod 2 & \text{if } \pi \equiv 5, 7 \mod 8 \\ \equiv d_2(E/\mathbb{Q}) \mod 2 & \text{if } \pi \equiv 1, 3 \mod 8 \end{cases}$$

If $2|n$ then $$d_2(E_\pi/\mathbb{Q}) \begin{cases} \not\equiv d_2(E/\mathbb{Q}) \mod 2 & \text{if } \pi \equiv 3, 7 \mod 8 \\ \equiv d_2(E/\mathbb{Q}) \mod 2 & \text{if } \pi \equiv 1, 5 \mod 8 \end{cases}$$

Chapter 4

Additional changes to 2-Selmer rank

The next proposition shows how to simultaneously increase the 2-Selmer rank of finitely many elliptic curves or just one of them.

Proposition 4.0.3. *Let $E^1, \dots, E^n$ be elliptic curves with rational 2-torsion. Let $S \supseteq \cup S(E^i)$ be a finite set of places of K and let $\mathfrak{p} = (\pi)$ be a prime ideal not in S such that $\pi \in K^\times$ and $\pi \in {K_v^\times}^2$ for all $v \in S$. Then for $i = 1, \dots, n$,*

$$d_2(E^i_\pi/K) = d_2(E^i/K) + 2.$$

Suppose each E^i has a distinct place of additive reduction, $\mathfrak{q}_i$ (see Definition 1.1.4). Let $\mathfrak{p} = (\pi)$ be a prime ideal not in S such that $\pi \in K^\times$ and $\pi \in {K_v^\times}^2$ for all $v \in S \backslash \{\mathfrak{q}_2, \dots, \mathfrak{q}_n\}$ and $\left(\frac{\pi}{\mathfrak{q}_i}\right) = -1$, for $i = 2, \dots, n$. Then

$$d_2(E^1_\pi/K) = d_2(E^1/K) + 2 \qquad d_2(E^i_\pi/K) = d_2(E^i/K), i > 1.$$

Proof. Let $E = E^i$, $F = K(\sqrt{\pi})$ and $T = \{\mathfrak{p}\}$. All places outside of T are split so the local condition doesn't change there. By Lemma 2.2.1 we again conclude that $H^1_f(K_\mathfrak{p}, E[2]) \cap H^1_f(K_\mathfrak{p}, E^F[2]) = 0$. Therefore we have satisfied all the requirements of Proposition 2.1.1.

Then the proposition says that

$$\mathrm{d}_2(E^F/K) = \mathrm{d}_2(E/K) - \dim V_T + \dim V_T^F.$$

With the restriction that

$$\dim V_T + \dim V_T^F \leq \dim \sum_{v \in T} H^1_f(K_v, E[2]) = 2. \tag{4.1}$$

We see that $\mathrm{loc}_{\mathfrak{p}} : \mathrm{Sel}_2(E^F/K) \twoheadrightarrow H^1_f(K_{\mathfrak{p}}, E^F[2])$ is surjective because of the image of the 2-torsion. Hence $\dim V_T^F \geq 2$, combining this with (4.1) shows that $\dim V_T^F = 2$ and $\dim V_T = 0$.

The second statement follows from the above proof and Proposition 2.2.7. □

Proposition 4.0.4. *Let $E^1, \ldots, E^n$ be elliptic curves over K with rational 2-torsion and suppose K has a real place v_∞. Let $S \supseteq \cup S(E^i)$ be a finite set of places of K and let $\mathfrak{p} = (\pi)$ be a prime ideal not in S such that $\pi \in K^\times$ and $\pi \in K_v^{\times 2}$ for all $v \in S \backslash \{v_\infty\}$ and π is not a square at v_∞. Then for $i = 1, \ldots, n$,*

$$d_2(E^i_\pi/K) \not\equiv d_2(E^i/K) \mod 2.$$

Proof. Let $E = E^i$. The parity of $d_2(E/K) + d_2(E_\pi/K)$ is equal to the parity of the rank of the 2-Selmer group of E over $K(\sqrt{\pi})$ [Monsky, 1996, Lemma 1.2]. The parity of this rank is the same as the parity of the sum $\sum i_v(E/K(\sqrt{\pi}))$ [Kramer, 1981, Theorem 1], where the $i_v(E/K(\sqrt{\pi}))$ is the local norm index as defined in [Kramer, 1981].

If v is unramified in a quadratic extension, F/K and v is a place of good reduction for E, then [Kramer, 1981, pg.123] shows that $i_v(E/F) = 0$. Hence,

$$d_2(E/K) + d_2(E_\pi/K) \equiv \sum_{v \in S(E) \cup \{\mathfrak{p}\}} i_v(E/K(\sqrt{\pi})) \mod 2.$$

For the places $\mathfrak{q} \in S(E) \backslash \{v_\infty\}$, we see $\pi \in K_{\mathfrak{q}}^{\times 2}$ hence $i_{\mathfrak{q}} = 0$. Furthermore, $i_{v_\infty} = 1$ by [Kramer, 1981, pg. 128] and $i_{\mathfrak{p}} = 0$ by [Kramer, 1981, Proposition 3].

□

Theorem 4.0.5. *Let $E^1, \ldots, E^n$ be elliptic curves over K with rational 2-torsion such that each elliptic curve has a distinct place of additive reduction. Let $a \in K^\times$ be such that $E^1_a, \ldots, E^n_a$ have 1-dimensional restricted 2-Selmer group (e.g. see Lemma 2.2.2).*

- *Suppose that the elliptic curves, $E^1_a, \ldots, E^n_a$, have the same 2-Selmer rank parity. If K has a real place, then there exist infinitely many $b \in K^\times$ such that the quadratic twists $E^1_{ab}, \ldots, E^n_{ab}$ all have essential 2-Selmer rank one. If each elliptic curve has odd 2-Selmer rank parity then the assumption on K is not necessary.*

- *Let $(k_1, \ldots, k_n)$ be an n-tuple of integers such that $k_i \equiv \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^i_a/K) \mod 2$ and $k_i \geq 2$. Then there exist infinitely many $b \in K^\times$ such that $\dim_{\mathbb{F}_2} \mathrm{Sel}(E^i_{ab}/K) = k_i$.*

Proof. Let $E_a^1, \ldots, E_a^n$ be as in the theorem.

For the first statement, if each E_a^i has the same 2-Selmer rank parity and the parity is odd, then Theorem 3.2.5 above gives a single $b \in K^\times$ such that E_{ab}^i has essential 2-Selmer rank one, for $i = 1, \ldots, n$. If the parity is even then the real place allows us to use Proposition 4.0.4, which gives a $b' \in K^\times$ such that the 2-Selmer rank parity of each $E_{ab'}^i$ is odd. Then we are in the situation of the first part of this paragraph.

The second part follows from the first part and Proposition 4.0.3. By Theorem 3.2.5 there exists a $b' \in K^\times$ such that the essential 2-Selmer rank of $E_{ab'}^i$ is either zero or one and is congruent to $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_a^i/K)$ modulo 2. Then apply Proposition 4.0.3 to increase the 2-Selmer rank as needed, since this only increase the 2-Selmer rank by an even number the parity does not change. □

Chapter 5

Hasse Principle for certain K3 surfaces

Recall that we are interested in the Hasse Principle for the family of K3 surfaces

$$Z^2 = f(X)g(Y), \tag{5.1}$$

where $f(X), g(Y)$ are quartic polynomials with no repeated roots. By the Hasse Principle we simply mean: if (5.1) has a local solution for every completion of K then it also has a K-rational solution. A solution to equation (5.1) is equivalent to a solution to both

$$D_a^1 : Z_1^2 = af(X) \text{ and } D_a^2 : Z_2^2 = ag(Y), \tag{5.2}$$

for some $a \in K^\times$. In this notation, D_a^i is the quadratic twists of $D^i := D_1^i$ by $\mathbb{Q}(\sqrt{a})$. Hence if we assume that (5.1) has a local solution for every place of K, we get an $a_v \in K_v^\times$ such that both

$$Z_1^2 = a_v f(X) \text{ and } Z_2^2 = a_v g(Y)$$

have a solution in K_v. The Hasse principle is then equivalent to finding an $a \in K^\times$ such that (5.2) has a solution in K. Recall that E^1, E^2 are the Jacobians of D^1, D^2 and we assume that E^1, E^2 have K-rational 2-torsion, see Theorem 6.0.7.

Recall that if D^i is everywhere locally soluble it can be viewed as an element of the 2-Selmer group of E^i, and is given by $m^{(i)} = (m_1^{(i)}, m_2^{(i)}, m_3^{(i)})$, under the embedding $\mathrm{Sel}_2(E^i/K) \subset (K^\times/K^{\times 2})^3$ from Chapter 2.

Note that if we twist both D_a^1 and D_a^2 by $K(\sqrt{b})$ the resulting 2-coverings are D_{ab}^1 and D_{ab}^2. Hence if the twisted 2-coverings have solutions over K, then (5.1) will also have a solution over K.

The goal is then to find a quadratic twist, $b \in K^\times$, such that $D_{ab}^i \in \mathrm{Sel}_2(E_{ab}^i/K)$ and the essential 2-Selmer rank of E_{ab}^i is one, for $i = 1, 2$. Then if we assume that the Shafarevich-Tate group of both E_{ab}^i is finite, the Cassels-Tate pairing will be a perfect pairing of finite groups. Thus the 2-primary torsion of $Ш(E_{ab}^i)$ has square cardinality and is thus trivial. This implies that both D_{ab}^i are trivial in the Shafarevich-Tate group and hence have solutions over K.

Remark 5.0.6. We can make the above process *unconditional* if both elliptic curves are the congruent number elliptic curve, $y^2 = x^3 - n^2x$, and satisfy the conditions of Theorem 6.0.7 below. This includes significantly more K3 surfaces than the family in Theorem 1.1.1. We explain the process in detail, in the proof of Theorem 1.1.1 below.

Chapter 6

The congruent number elliptic curve over $\mathbb{Q}$

We want to consider the special case where both E^1 and E^2 are different twists of $y^2 = x^3 - x$. Say $E^1 : y^2 = x^3 - n_1^2 x$ and $E^2 : y^2 = x^3 - n_2^2 x$.

Let $P_r(n)$ be the condition that n has at most r prime factors congruent to $3 \mod 4$. Let $Q_r(n)$ be the condition that n has at most r prime factors congruent to $\pm 3 \mod 8$.

Theorem 6.0.7. *[Tian and Zhang, 2013, Corollary 1.4] Let n be an integer such that the class group of $\mathbb{Q}(\sqrt{-n})$ has no elements of order 4. If n also satisfies one of the congruence conditions below, then the elliptic curve $y^2 = x^3 - n^2 x$ has Mordell-Weil rank one and finite Shafarevich-Tate group:*

- $n \equiv 5 \mod 8$ *and n has property $P_0(n)$ or $Q_1(n)$*
- $n \equiv 7 \mod 8$ *and n has property $P_1(n)$ or $Q_0(n)$*

The condition is explicit in terms of the parity of the genus class numbers of divisors of n, where the genus class number, $g(d)$, is the order of the group $2Cl(\mathbb{Q}(\sqrt{-d}))$.

6.1 Genus class numbers

We would like to find an infinite class of integers, n, such that they both satisfy the congruence conditions of Theorem 6.0.7 and the class group of $\mathbb{Q}(\sqrt{-d})$ has no elements of order 4. Following

[Tian and Zhang, 2013], let $g(n)$ be the order of two times the class group of $\mathbb{Q}(\sqrt{-n})$. Notice that $g(n)$ is odd if and only if the 4-rank of the class group of $\mathbb{Q}(\sqrt{-d})$ is zero.

Following the work of Rédei, see [Kolster, 2005, pg. 81] for the version stated below, we can compute the 4-rank of the class group of quadratic number fields by computing the rank of a matrix of Hilbert symbols. He shows that for $\mathbb{Q}(\sqrt{-d})/\mathbb{Q}$, if p_i for $i = 1 \dots k$ are the primes that ramify in the extension and

$$M' = \begin{pmatrix} (p_1,d)_{p_1} & (p_1,d)_{p_2} & \dots & (p_1,d)_{p_k} \\ (p_2,d)_{p_1} & (p_2,d)_{p_2} & \dots & (p_2,d)_{p_k} \\ \vdots & & \ddots & \vdots \\ (p_k,d)_{p_1} & (p_k,d)_{p_2} & \dots & (p_k,d)_{p_k} \end{pmatrix}.$$

Then $\operatorname{rank}_4(Cl(\mathbb{Q}(\sqrt{-d}))) = k - 1 - \operatorname{rank}(M')$.

Proposition 6.1.1. *Let E be the congruent number elliptic curve $y^2 = x^3 - n^2x$. If $d_2(E/\mathbb{Q}) = 3$ and $n \equiv 7 \mod 8$ and n satisfies $Q_0(n)$, then E satisfies the conditions of Theorem 6.0.7.*

Proof. Let n be as above, then it satisfies the congruence conditions of Theorem 6.0.7 and thus it only remains to show that $g(n)$ is in fact odd.

In the appendix of [Heath-Brown, 1994] Monsky shows that the 2-Selmer rank of E is related to the rank of a matrix. Namely, he shows that $d_2(E/\mathbb{Q}) - 2 = 2k - \operatorname{rank}(M)$ and $d_2(E/\mathbb{Q}) - 2 = \begin{cases} 2k - \operatorname{rank}(M_2) & \text{if } n \equiv 1 \mod 4 \\ 2k - 1 - \operatorname{rank}(M_2) & \text{if } n \equiv 3 \mod 4 \end{cases}$.

Here

$$M = \begin{pmatrix} A + D_2 & D_2 \\ D_2 & A + D_{-2} \end{pmatrix} \text{ and } M_2 = \begin{pmatrix} A + A^T & A^T \\ A & D_2 \end{pmatrix},$$

where D_k is the diagonal matrix with $\left(\frac{k}{p_i}\right)$ along the diagonal and A^T is the Rédei matrix M' above (when $n \equiv 3 \mod 4$), used to compute the 4-rank of the class group of $\mathbb{Q}(\sqrt{-n'})$.

Let $n \equiv 7 \mod 8$ satisfying $Q_0(n)$. Then $D_2 = 0$ since all the prime factors of n are congruent to ± 1 modulo 8. Then M_2 is equivalent to $\begin{pmatrix} A^T & A^T \\ A & 0 \end{pmatrix}$. Since the essential 2-Selmer rank of E is one we have $2k - 2 = 2\operatorname{rank}(A)$. Thus $\operatorname{rank}(A) = k - 1$, meaning that $g(n)$ is odd. □

Hence by applying the reduction process to the congruent number elliptic curves we unconditionally get the Hasse Principle for these K3 surfaces (i.e. we do not need to assume that the

Shafarevich-Tate group is finite).

6.2 Proof of the main theorems

The proof of Theorem 1.1.1 is very similar to the process described in Chapter 5, but here the elliptic curves do not have places of multiplicative reduction.

Proof of Theorem 1.1.1. We consider the K3 surface

$$Z^2 = \left(a - \frac{n^2}{a}X^4\right)\left(b - \frac{m^2}{b}Y^4\right), \tag{6.1}$$

where $a|n$ and $b|m$ and $a \nmid m$ and $b \nmid n$. Note that this is a more general setting than the hypothesis of the theorem, but we will impose the additional conditions later.

In the notation of the paper, the surface (6.1) gives the two quartics, $f : Z_1^2 = a - \frac{n^2}{a}X^4$ and $g : Z_2^2 = b - \frac{m^2}{b}Y^4$. The Jacobians of the quartics f and g are the elliptic curves $E^1 : y^2 = x^3 - 4n^2x$ and $E^2 : y^2 = x^3 - 4m^2x$, respectively. Recall that one of the assumptions of the theorem is that f, g are everywhere locally soluble. Furthermore, an explicit computation shows that the quartic f corresponds to the triple $m^{(1)} := (a, 1, a) \in \mathrm{Sel}_2(E^1/\mathbb{Q})$ (under the embedding $\mathrm{Sel}_2(E^1/\mathbb{Q}) \subset (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^3$, see Chapter 2) and similarly the quartic g corresponds to the triple $m^{(2)} := (b, 1, b) \in \mathrm{Sel}_2(E^2/\mathbb{Q})$. Then we can very explicitly describe the Hasse principle for this K3 surface. We now impose the following assumptions:

1. E^1, E^2 have distinct additive places. Hence, $m \nmid n$ and $n \nmid m$ (i.e. $\gcd(m, n) \notin \{m, n\}$).

2. Any triple (m_1, m_2, m_3) (not equal to $m^{(1)}, m^{(2)}$) with each m_i only in the subgroup generated by the divisors of a and b is not locally solvable in some $\mathbb{Q}_p$. Furthermore, $D^1 := f$ and $D^2 := g$ are everywhere locally soluble, when viewed as 2-coverings of E^i, for $i = 1, 2$.

3. $m^{(i)}$ is a unit at (one of) the distinct places coming from assumption 1, for $i = 1, 2$. In addition, $a \neq n$ and $b \neq m$.

Remark 6.2.1. Assumptions 1 and 3 are equivalent to: $\gcd(n/a, m) \neq n/a$, $\gcd(m/b, n) \neq m/b$.

Remark 6.2.2. Suppose $a = p$ and $b = q$ are both primes such that $p \nmid m$, $q \nmid n$ and $p, q \equiv 3 \mod 4$ then assumption 2 holds using Monsky's conditions. In [Heath-Brown, 1994, Appendix],

Monsky states explicit conditions for a triple ($(p, 1, p)$ corresponds to $(a, b) = (1, p)$ in Monsky's notation) to be in the 2-Selmer group. The hypothesis of the theorem imply that we are in this scenario.

We further assume that m, n satisfy either:

- $n \equiv 5 \mod 8$, satisfies $P_0(n)$ and $g(n)$ is odd.
- $n \equiv 5 \mod 8$, satisfies $Q_1(n)$ and $g(n)$ is odd.
- $n \equiv 7 \mod 8$ and satisfies $Q_0(n)$.
- $n \equiv 7 \mod 8$ and satisfies $P_1(n)$ and $g(n)$ is odd.

(two of the congruence conditions in Theorem 6.0.7). Recall that by Monksy's proof of the parity conjecture for the congruent number problem, the two cases of Theorem 6.0.7 that we chose correspond to elliptic curves with odd 2-Selmer rank.

The second part of Assumption two assumes that both D^i are everywhere locally soluble, hence D^i is an element of $\mathrm{Sel}_2(E^i/\mathbb{Q})$ for $i = 1, 2$.

Assumption two implies that the hypotheses of Lemma 2.2.5 are satisfied, hence there exists a $b_1 \in \mathbb{Z}$ such that both $E^i_{b_1}$ have restricted 2-Selmer groups consisting of $D^i_{b_1}$ and the identity element. Since b_1 is a unit at the bad places of E^1 and E^2, the three assumptions above still hold for $E^i_{b_1}$ and the elliptic curves still satisfy the congruence conditions from Theorem 6.0.7.

Next we need a $b_2 \in \mathbb{Z}$ such that $E^i_{b_1 b_2}$ has essential 2-Selmer rank one. In order to apply Theorem 3.2.5 (with the restricted 2-Selmer group described above) to $E^i_{b_1}$, we need assumptions one and three and that the essential 2-Selmer rank is at least two. If the essential 2-Selmer rank is one, then we are already done, otherwise we can apply the theorem. Hence there exists a $b_2 \equiv 1 \mod 8$ such that both the elliptic curves $E^i_{b_1 b_2}$, for $i = 1, 2$, have essential 2-Selmer rank one (generated by $D^i_{b_1 b_2}$). Let $b = b_1 b_2$.

Hence $D^i_b \in \mathrm{Sel}_2(E^i_b/\mathbb{Q})$ for $i = 1, 2$ and both E^i_b have essential 2-Selmer rank one. Then E^1_b, E^2_b satisfy the conditions of Theorem 6.0.7 (in the third case, by Proposition 6.1.1), both E^1_b, E^2_b have Mordell-Weil rank one and finite Shafarevich-Tate group. Then the Cassels-Tate pairing is a perfect pairing of finite groups. Thus the 2-primary torsion of $Ш(E^i_b/K)$ has square cardinality and thus

$Ш(E_b^i/K)[2] = 0$. This implies that both D_b^i are trivial in the Shafarevich-Tate group and hence have a solution over $\mathbb{Q}$.

In summary, if $a = p$, $b = q$ are prime numbers congruent to 3 mod 4 and $m, n \in \mathbb{Z}$ such that $\gcd(n/p, m) \neq n/p$ and $\gcd(m/q, n) \neq m/q$ and f, g are everywhere locally soluble, then the three assumptions above are satisfied. Suppose both m, n satisfy one of the following conditions:

- $n \equiv 5 \mod 8$, satisfies $P_0(n)$ and $g(n)$ is odd.
- $n \equiv 5 \mod 8$, satisfies $Q_1(n)$ and $g(n)$ is odd.
- $n \equiv 7 \mod 8$ and satisfies $Q_0(n)$.
- $n \equiv 7 \mod 8$, satisfies $P_1(n)$ and $g(n)$ is odd.

Then,

$$Z^2 = \left(p - \frac{n^2}{p}X^4\right)\left(q - \frac{m^2}{q}Y^4\right), \tag{6.2}$$

has a solution over $\mathbb{Q}$. □

Proof of Theorem 1.1.2. For Theorem 1.1.2 to follow from Theorem 1.1.1 we need to show that if $P(n, p)$ and $P(m, q)$ are satisfied then the two 2-coverings $f : Z_1^2 = p - \frac{n^2}{p}X^4$ and $g : Z_2^2 = q - \frac{m^2}{q}Y^4$ are everywhere locally soluble, using the notation of the above proof. As above we note that f, g correspond to the triples $(p, 1, p)$ for E^1 and $(q, 1, q)$ for E^2, respectively. In [Heath-Brown, 1994, Appendix], Monsky states explicit conditions for a triple ($(p, 1, p)$ corresponds to $(a, b) = (1, p)$ in Monsky's notation) to be in the 2-Selmer group. These conditions translate exactly to $P(n, p)$ for $(p, 1, p)$ to be in $\mathrm{Sel}_2(E^1/\mathbb{Q})$ and to $P(m, q)$ for $(q, 1, q)$ to be in $\mathrm{Sel}_2(E^2/\mathbb{Q})$. □

6.3 More general examples

In the above examples we started with two elliptic curves that already had odd 2-Selmer rank parity, but this method can also deal with more general situations. If both E^1, E^2 have even 2-Selmer rank parity then use the real place of $\mathbb{Q}$ and Proposition 4.0.4 to change the parity. If only one of E^1 and E^2 has even 2-Selmer rank parity then use Corollary 3.3.2.

In order to use Corollary 3.3.2 to change the 2-Selmer rank (parity) without changing the chosen 2-covering we need to assume that 2 does not divide the $m_j^{(i)}$. We summarize the additional conditions in the following,

- If the 2-Selmer ranks of E^1, E^2 have the same parity then no additional assumptions are necessary. Apply Proposition 4.0.4 if they have even 2-Selmer rank parity.
- If exactly one of the elliptic curves has even 2-Selmer rank parity then assume $2 \nmid m_j^{(i)}$ for $i = 1, 2$ and $j = 1, 2, 3$ and either n or m has even valuation at 2 and the other has odd valuation at 2.

Part II

The Hasse Principle, conditionally

Chapter 7

Introduction

In this part we generalize the result of Skorobogatov and Swinnerton-Dyer to elliptic curves that have a multiplicative place. This allows us to remove some of the conditions in their paper, but the results in this part are all dependent on knowing that the Shafarevich-Tate group is finite.

Given finitely many elliptic curves with distinct places of multiplicative reduction and an element of the 2-Selmer group (an everywhere locally soluble 2-covering) for each elliptic curve, we describe sufficient conditions to find a single quadratic twist such that the 2-Selmer groups of the twisted elliptic curves are 3-dimensional (generated by the 2-covering and the image of the 2-torsion).

We recall some definitions from Part 1.

Definition 7.0.1. Let E be an elliptic curve over a number field K. The essential 2-Selmer rank of E is

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E/K) - \dim_{\mathbb{F}_2} E[2](K).$$

Definition 7.0.2. Let $E^1, \ldots, E^n$ be elliptic curves over K. Then a place, v, of K is a distinct place of bad (additive, multiplicative) reduction for E^i if v is a place of bad (additive, multiplicative) reduction for E^i and a place of good reduction for all E^j, $j \neq i$.

For an elliptic curve E over K and a quadratic extension F/K, the quadratic twist of E by F is denoted by E^F or if $F = K(\sqrt{b})$ then by E_b.

Given finitely many elliptic curves over K with rational 2-torsion, satisfying some mild hypotheses, we find a single quadratic extension such that each twisted elliptic curve has analytic rank bounded below by 1, see Theorem 7.1.2. Under the same conditions, we find a single quadratic

extension such that each twisted elliptic curve has 2-Selmer rank equal to three. If we further assume the finiteness of the Shafarevich-Tate groups (of the twisted elliptic curves) then each elliptic curve has Mordell-Weil rank one. If $K = \mathbb{Q}$, then under the above assumptions the analytic rank of each elliptic curves is one, see Corollary 7.1.3. Furthermore, with the assumption on the Shafarevich-Tate group (and $K = \mathbb{Q}$), we describe a single quadratic twist such that each elliptic curve has analytic rank zero and Mordell-Weil rank zero, again under some mild assumptions.

Given finitely many elliptic curves with distinct multiplicative and additive places (see Definition 1.1.4), we describe a single quadratic twist such that their 2-Selmer ranks are a prescribed pair of integers. This would give one twist which changes the 2-Selmer ranks of each elliptic curve to a chosen parity. A more general version of these statements is stated below for elliptic curves with rational 2-torsion, but there we can't (necessarily) change the parity, see Theorem 4.0.5.

Theorem 7.0.3. *Let $E^1, \dots, E^n$ be elliptic curves over K with rational 2-torsion such that each elliptic curve has a distinct place of multiplicative reduction and non-zero essential 2-Selmer rank. Then there exist infinitely many $b \in K^\times$ such that*

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_b^1) \leq \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^1) - 1 \quad \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_b^i) \leq \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^i), i > 1.$$

Furthermore $\dim \mathrm{Sel}_2(E_b^1) \not\equiv \dim \mathrm{Sel}_2(E^1) \mod 2$.

7.1 A few corollaries

Corollary 7.1.1. *Let $E^1, \dots, E^n$ be elliptic curves over K with rational 2-torsion such that each elliptic curve has a distinct place of multiplicative reduction. Then there exist infinitely many $b \in K^\times$ such that the quadratic twists $E_b^1, \dots, E_b^n$ each have essential 2-Selmer rank one. In addition, there exist infinitely many $c \in K^\times$ such that the quadratic twists $E_c^1, \dots, E_c^n$ each have essential 2-Selmer rank 0 (in particular Mordell-Weil rank 0 and $Ш(E_c^i/K)[2] = 0$).*

Theorem 7.1.2. *Let $E^1, \dots, E^n$ be elliptic curves over K with rational 2-torsion such that each elliptic curve has a distinct place of multiplicative reduction. Then there exist infinitely many $b \in K^\times$ such that the analytic rank of each E_b^i over K is at least one.*

Proof. Apply Corollary 7.1.1 to get infinitely many b such that the essential 2-Selmer rank of each

E_b^i is one. We have the exact sequence

$$0 \to E(K)[p] \to \mathrm{Sel}_p(E/K) \to \mathrm{Sel}_{p^\infty}(E/K)[p] \to 0, \tag{7.1}$$

where $\mathrm{Sel}_{p^\infty}(E/K)$ is the p^∞-Selmer group and $[p]$ denotes the p-torsion. Then using the Cassels-Tate pairing and the above exact sequence we see that if the essential 2-Selmer rank is one then the essential 2^∞-Selmer rank is one.

Recall that the p-parity conjecture relates the p^∞-Selmer rank with the root number of the elliptic curve, see [Dokchitser and Dokchitser, 2011] for a definition of the root number. It is proved in some cases, in particular when $p = 2$, K is a number field and there is a rational 2-isogeny, see [Dokchitser and Dokchitser, 2011]. Thus the root number of each E_b^i is -1, hence the lower bound on the analytic rank. □

Corollary 7.1.3. *Let $E^1, \ldots, E^n$ be elliptic curves over $\mathbb{Q}$ with rational 2-torsion such that each elliptic curve has two distinct places of multiplicative reduction.*

1. *Let $b \in \mathbb{Q}^\times$ be such that $E_b^1, \ldots, E_b^n$ each have essential 2-Selmer rank one (e.g. from Corollary 7.1.1). If the Shafarevich-Tate group of each of $E_b^1, \ldots, E_b^n$ is finite, then $E_b^1, \ldots, E_b^n$ each have analytic rank one and Mordell-Weil rank one.*

2. *Similarly, let $c \in \mathbb{Q}^\times$ be such that $E_c^1, \ldots, E_c^n$ each have essential 2-Selmer rank zero (e.g. from Corollary 7.1.1). If the Shafarevich-Tate group of each of $E_c^1, \ldots, E_c^n$ is finite, then $E_c^1, \ldots, E_c^n$ each have analytic rank zero and Mordell-Weil rank zero.*

Remark 7.1.4. The assumption on the Shafarevich-Tate group can already be reduced to knowing that the 2-primary and p-primary components are finite (for one large p), but we expect it to be removed completely. This follows from the proof below, since the results quoted there only need one good enough prime.

Proof. We use a recent result due to Zhang [Zhang, 2013] and in the square-free conductor case independently due to Skinner [Skinner, 2013]. Zhang proves a converse to the result of Gross-Zagier and Kolyvagin, [Zhang, 2013, Theorem 1.5]: Given an elliptic curve over $\mathbb{Q}$ with two places of multiplicative reduction, he shows that if the Mordell-Weil rank is one and the Shafarevich-Tate group is finite then the analytic rank is one. Let $E_b^1, \ldots, E_b^n$ be as in the theorem. If $Ш(E_b^i/\mathbb{Q})[2^\infty]$ is finite

then the Cassels-Tate pairing shows that $Ш(E_b^i/\mathbb{Q})[2^\infty]$ has square order, and thus $Ш(E_b^i/\mathbb{Q})[2] = 0$ and the Mordell-Weil rank of E_b^i is one. Then applying Zhang's theorem gives the desired result.

For the second part, let $E_c^1, \ldots, E_c^n$ be as in the theorem. We use a result of Skinner and Urban on the main conjecture [Skinner and Urban, 2014, Theorem 2 (b)]: Given an elliptic curve over $\mathbb{Q}$, they show that if p^∞-Selmer group is finite for a 'good' prime p then the analytic rank is zero. If $Ш(E_c^i/\mathbb{Q})[2^\infty]$ is finite then the Cassels-Tate pairing shows that $Ш(E_c^i/\mathbb{Q})[2^\infty]$ has square order, and thus $Ш(E_c^i/\mathbb{Q})[2] = 0$ and the Mordell-Weil rank of E_c^i is zero. Then choose a large enough prime, p, such that $Ш(E_c^i/\mathbb{Q})[p] = 0$ for all i, again by the finiteness of the Shafarevich-Tate groups. This prime p can be chosen to be a 'good' prime as above, since their conditions are satisfied for infinitely many primes (the first condition holds for infinitely many p, the second condition holds for large p, by Serre's theorem, and the third condition holds for infinitely many p by [Silverman, 1994, Prop V.6.1, Ex. V.5.13, Rmk. IV.9.6]). Then the p-Selmer group for each E_c^i is trivial since the Mordell-Weil rank is zero, E_c^i doesn't have $\mathbb{Q}$-rational p-torsion (since $p > 11$) and the p-torsion of the Shafarevich-Tate group is trivial. By (7.1) this implies that $\mathrm{Sel}_{p^\infty}(E_c^i/\mathbb{Q})[p] = 0$. We know that $\mathrm{Sel}_{p^\infty}(E_c^i/\mathbb{Q}) = (\mathbb{Q}_p/\mathbb{Z}_p)^r \oplus \text{finite}$. Then since the $\mathbb{Q}$-rational p-torsion of E^i is trivial, $\mathrm{Sel}_{p^\infty}(E_c^i/\mathbb{Q}) = 0$. Applying Skinner-Urban's result gives the desired conclusion. □

Corollary 7.1.5. *Let $E^1, \ldots, E^n$ be elliptic curves over K with rational 2-torsion such that each elliptic curve has a distinct place of multiplicative reduction. If we further assume that the 2-primary part of the Shafarevich-Tate group of the twisted elliptic curves is finite. Then there exist infinitely many $b \in K^\times$ such that $E_b^1, \ldots, E_b^n$ each have Mordell-Weil rank 1 and the 2-torsion part of their Shafarevich-Tate group is trivial.*

Proof. By Corollary 7.1.1 there exists a $b \in K^\times$ such that $E_b^1, \ldots, E_b^n$ each have essential 2-Selmer rank 1. If $Ш(E/K)[2^\infty]$ is finite then the Cassels-Tate pairing shows that $Ш(E/K)[2^\infty]$ has square order, and thus $Ш(E/K)[2] = 0$. □

Corollary 7.1.6. *Let $E^1, \ldots, E^n$ be elliptic curves over K with rational 2-torsion such that each elliptic curve has distinct places of additive and multiplicative reduction. Let $(k_1, \ldots, k_n)$ be an n-tuple of integers, then there exist infinitely many $b \in K^\times$ such that $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_b^i/K) = k_i$. In particular we can choose the parity of each 2-Selmer group.*

Proof. Outline: Reduce the 2-Selmer ranks to either zero or one depending on the parity of k_i using Proposition 7.1.1 and then increase the 2-Selmer rank of each elliptic curve to k_i using Proposition 4.0.3. □

Chapter 8

Elliptic Curves with Multiplicative Reduction

Throughout this Chapter E is an elliptic curve with a multiplicative place.

The next lemma allows us to change the parity of the 2-Selmer groups and follows from [Kramer, 1981]. The version below shows that consecutive twists, $(E_c)_b$, do not have to be squares at the additive places, $v|c$, introduced by the previous twist. It allows us to control the local condition at an additive place, the lemma is stated in [Skorobogatov and Swinnerton-Dyer, 2005].

Lemma 8.0.7. *[Skorobogatov and Swinnerton-Dyer, 2005, Lemma 5] Let E_b be a twisted elliptic curve and let $\mathfrak{p}_1$ be a place of multiplicative reduction for E. Let $c \in K^\times$ be such that c is a unit at all places $\mathfrak{q}|b$, $b \in K_\mathfrak{q}^{\times 2}$ for all $\mathfrak{q} \in S(E)\backslash\{\mathfrak{p}_1\}$ and $\left(\frac{c}{p_1}\right) = -1$. Then $d_2(E_{cb}/K)$ and $d_2(E_b/K)$ have opposite parities.*

Proof. The parity of $d_2(E/K) + d_2(E_b/K)$ is equal to the parity of the rank of the 2-Selmer group of E over $K(\sqrt{b})$ [Monsky, 1996, Lemma 1.2] . The parity of this rank is the same as the parity of the sum $\sum i_v(E/K(\sqrt{b}))$ [Kramer, 1981, Theorem 1], where the $i_v(E/K(\sqrt{b}))$ is the local norm index as defined in [Kramer, 1981].

If v is unramified in a quadratic extension, F/K and v is a place of good reduction for E, then [Kramer, 1981, pg.123] shows that $i_v(E/F) = 0$. Hence,

$$d_2(E/K) + d_2(E_b/K) \equiv \sum_{S(E)\cup\{v|b\}} i_v(E/K(\sqrt{b})) \mod 2$$

and similarly,

$$d_2(E/K) + d_2(E_{cb}/K) \equiv \sum_{S(E)\cup\{v|cb\}} i_v(E/K(\sqrt{cb})) \mod 2.$$

Since b is a unit at all places $\mathfrak{q}|c$, neither the reduction type of E at $\mathfrak{q}$ nor whether $\mathfrak{q}$ is ramified in $K(\sqrt{cb})/K$ will change, hence $i_\mathfrak{q}(E/K(\sqrt{cb})) = i_\mathfrak{q}(E/K(\sqrt{b}))$ for $\mathfrak{q}|b$.

Therefore,

$$d_2(E_{cb}/K) \equiv d_2(E_b/K) + \sum_{S(E)\cup\{v|c\}} i_v(E/K(\sqrt{cb})) \mod 2.$$

For the places $\mathfrak{q} \in S(E)\backslash\{\mathfrak{p}_1\}$, we see $c \in K_\mathfrak{q}^{\times 2}$ hence $i_\mathfrak{q} = 0$.

The extension $K_{\mathfrak{p}_1}(\sqrt{cb})/K_{\mathfrak{p}_1}$ is unramified thus $i_{\mathfrak{p}_1} = 1$ by [Kramer, 1981, Propositions 1 and 2].

For a prime $\mathfrak{q}$ dividing c to an odd power we see that the extension $K_\mathfrak{q}(\sqrt{cb})/K_\mathfrak{q}$ is ramified and E has good reduction at $\mathfrak{q}$, hence $i_\mathfrak{q} = 0$ by [Kramer, 1981, Proposition 3]. □

Proposition 8.0.8. *Let E_c be a twisted elliptic curve with E as above. Let $\mathfrak{p}_1$ be a multiplicative place for E and $\mathfrak{q}_0$ be a prime ramified in $K(\sqrt{c})/K$ such that $\mathfrak{p}_1, \mathfrak{q}_0$ satisfy Lemma 2.2.6. Let $\mathfrak{p} = (\pi)$ be a prime such that $\pi \in K_\mathfrak{q}^{\times 2}$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{q}_0, \mathfrak{p}_1\}$ with $S \supseteq S(E_c)$ and $\left(\frac{\pi}{\mathfrak{q}_0}\right) = -1 = \left(\frac{\pi}{\mathfrak{p}_1}\right)$. Then either*

i $d_2(E_{c\pi}/K) = d_2(E_c/K) - 1$ *or*

ii $d_2(E_{c\pi}/K) = d_2(E_c/K) + 1$ *and* $\mathrm{loc}_{\mathfrak{q}_0,\mathfrak{p}}$ *is surjective.*

Furthermore the restricted 2-Selmer group does not change, if its elements are units at $\mathfrak{p}_1$.

Proof. Let $T = \{\mathfrak{p}_1, \mathfrak{q}_0, \mathfrak{p}\}$. The extension $F = K(\sqrt{\pi})/K$ is split for all places $v \notin T$ and hence the local condition $H^1_f(K_v, E_c[2])$ is the same for E_c and $E_{c\pi}$. Furthermore we know that the parity of $\dim \mathrm{Sel}_2(E_{c\pi}/K)$ and $\dim \mathrm{Sel}_2(E_c/K)$ is different by Lemma 8.0.7.

We use the more general version of Proposition 2.1.1. By [Skorobogatov and Swinnerton-Dyer, 2005, Lemma 4] we conclude that $H^1_f(K_v, E_c[2]) \cap H^1_f(K_v, E_c^F[2]) = 0$, when $v = \mathfrak{q}_0, \mathfrak{p}$ and $H^1_f(K_{\mathfrak{p}_1}, E_c[2]) \cap H^1_f(K_{\mathfrak{p}_1}, E_c^F[2])$ is 1-dimensional. Then the more general proposition says that

$$\mathrm{d}_2(E_c^F/K) = \mathrm{d}_2(E_c/K) - \dim V_T + \dim V_T^F,$$

with the restriction that

$$\dim V_T + \dim V_T^F \leq \sum_{v \in T} \dim H_f^1(K_v, E_c[2]) + 1 = 7. \tag{8.1}$$

We see that $\mathrm{loc}_{\mathfrak{p}_1,\mathfrak{q}_0} : \mathrm{Sel}_2(E_c/K) \twoheadrightarrow H_f^1(K_{\mathfrak{q}_0}, E_c[2]) \oplus H_f^1(K_{\mathfrak{p}_1}, E_c[2])$ is at least 3-dimensional by assumption. Similarly, $\mathrm{loc}_{\mathfrak{p}} : \mathrm{Sel}_2(E_c^F/K) \twoheadrightarrow H_f^1(K_{\mathfrak{p}}, E_c^F[2])$ is surjective because of the image of the 2-torsion. Hence $\dim V_T \geq 3$ and $\dim V_T^F \geq 2$.

Hence, by (8.1), the only possibilities for $(\dim V_T, \dim V_T^F)$ are $(3,2), (3,4)$ and $(4,3)$. Thus either the rank goes up by 1 or it drops by 1.

If V_T^F is 4-dimensional:

Since the image of the 2-torsion is surjective onto each 2-dimensional subspace, $H_f^1(K_v, E[2])$, we can translate both of the two 'new' vectors (not the image of the 2-torsion) to get vectors which fall into one of four types:

a) If it is trivial at $\mathfrak{p}$ and non-trivial at exactly one of $\mathfrak{q}_0$ or $\mathfrak{p}_1$ then it wouldn't satisfy the correct local condition at $\mathfrak{p}$, since it is not a square at $\mathfrak{p}$

b) If it is trivial at exactly one of $\mathfrak{q}_0, \mathfrak{p}_1$ and non-trivial at $\mathfrak{p}$ then it has the wrong condition at $\mathfrak{p}$, since the local condition there is $(1,1,1)$ and permutations of $(\pi, \pi, 1)$.

c) If it is trivial at $\mathfrak{q}_0$ and $\mathfrak{p}_1$ and not at $\mathfrak{p}$, or equivalently it is trivial at $\mathfrak{p}$ and non-trivial at $\mathfrak{q}_0, \mathfrak{p}_1$. These are potentially non-trivial.

d) If it is non-trivial in all three components, then $\mathrm{loc}_{\mathfrak{q}_0}$ and $\mathrm{loc}_{\mathfrak{p}_1}$ must be the image of the same 2-torsion element, otherwise it does not satisfy the correct condition at $\mathfrak{p}$. Therefore, any such vector is the image of the 2-torsion.

Thus the only way $\dim V_T^F = 4$ is if we have two (linearly independent) vectors of type c) above. Hence $\mathrm{loc}_{\mathfrak{p},\mathfrak{q}_0}$ is surjective for $E_{c\pi}$.

□

Theorem 8.0.9. *Let $E^1, E^2/K$ be elliptic curves with rational 2-torsion and let $\mathfrak{q}_1, \tilde{\mathfrak{q}_1}$ be distinct places of multiplicative reduction for E^1, E^2, respectively. Furthermore, let $b \in K^\times$ be such that E_b^1, E_b^2 have 1-dimensional restricted 2-Selmer group (e.g. see Lemma 2.2.2). Assume that the essential 2-Selmer rank of E_b^1 is at least one. Then there exist infinitely many $c \in K^\times$ such that,*

1. $\dim \mathrm{Sel}_2(E_{bc}^1) = \dim \mathrm{Sel}_2(E_b^1) - 1 \quad \dim \mathrm{Sel}_2(E_{bc}^2) \leq \dim \mathrm{Sel}_2(E_b^2)$.

2. *Furthermore, $c \in \mathcal{O}_{K_v}^{\times}$ for $v \in \cup S(E^i)$ and -1 is not a square at c. (In particular, c is a local square at all even primes of K. When $K = \mathbb{Q}$, this implies that $c \equiv 1 \mod 8$.)*

3. *The elements of the restricted 2-Selmer group of E_b^i which are units at $\mathfrak{q}_1$ are also in the restricted 2-Selmer group of E_{bc}^i.*

4. *If the 2-Selmer rank of E_b^i is odd, for $i = 1, 2$. Then there exist infinitely many $c \in K^{\times}$ such that the quadratic twists E_c^i each have essential 2-Selmer rank 1.*

Proof. By assumption the 2-Selmer group of E_b^1 has essential 2-Selmer rank at least 1, thus by Part 2 of Lemma 2.2.6, we get a $\mathfrak{q}_0$ such that $\mathrm{loc}_{\mathfrak{q}_0,\mathfrak{q}_1}$ is 3-dimensional. Now apply Proposition 8.0.8, where $S = \cup S(E_b^i)$, this gives a $c' \in K^{\times}$. If the 2-Selmer rank of $E_{bc'}^1$ is one less than the 2-Selmer rank of E_b^1 then let $c = c'$. If the 2-Selmer rank of $E_{bc'}^1$ is one greater than the 2-Selmer rank of E_b^1 then apply Proposition 3.1.1 using the primes given by the proposition, this give a $c'' \in K^{\times}$. Then let $c = c'c''$.

The 2-Selmer rank of E_b^2 is the same as the 2-Selmer rank of E_{bc}^2: The quadratic twist by c' changes the local condition at $\mathfrak{q}_0$ - a place of additive reduction for E_b^2 and at $\mathfrak{p}_1$ - a place of good reduction for E_b^2. Hence by Proposition 2.2.7 the 2-Selmer ranks of E_b^2 and E_{bc}^2 are the same. The quadratic twist by c'' does not increase the 2-Selmer rank of E^2 by Proposition 3.1.1.

Furthermore, $c \in {\mathcal{O}_{K_v}^{\times}}^2$ for $v \in \cup S(E^i) \setminus \{\mathfrak{q}_0, \mathfrak{q}_1, \}$ since this is the case for Propositions 8.0.8 and 3.1.1. Since $\mathfrak{q}_0 | b$ the quadratic twist does not effect the elements of the restricted 2-Selmer group which are units at $\mathfrak{q}_1$. Thus the restricted 2-Selmer group of E_b^i is a subgroup of $\mathrm{Sel}_2(E_{bc}^i/K)$.

The last statement follows by applying the first one repeatedly (this is possible by the second property) and changing the roles of E^1 and the E^2 as necessary. □

Chapter 9

Hasse Principle for certain K3 surfaces

Recall that we are interested in the Hasse Principle for the family of K3 surfaces

$$Z^2 = f(X)g(Y), \tag{9.1}$$

where $f(X), g(Y)$ are quartic polynomials with no repeated roots. By the Hasse Principle we simply mean: if (9.1) has a local solution for every completion of K then it also has a K-rational solution. A solution to equation (9.1) is equivalent to a solution to both

$$D_a^1 : Z_1^2 = af(X) \text{ and } D_a^2 : Z_2^2 = ag(Y), \tag{9.2}$$

for some $a \in K^\times$. In this notation, D_a^i is the quadratic twists of $D^i := D_1^i$ by $\mathbb{Q}(\sqrt{a})$. Hence if we assume that (9.1) has a local solution for every place of K, we get an $a_v \in K_v^\times$ such that both

$$Z_1^2 = a_v f(X) \text{ and } Z_2^2 = a_v g(Y)$$

have a solution in K_v. The Hasse principle is then equivalent to finding an $a \in K^\times$ such that (9.2) has a solution in K. Recall that E^1, E^2 are the Jacobians of D^1, D^2 and we assume that E^1, E^2 have K-rational 2-torsion, see Proposition 9.0.11.

Recall that if D^i is everywhere locally soluble it can be viewed as an element of the 2-Selmer group of E^i, and is given by $m^{(i)} = (m_1^{(i)}, m_2^{(i)}, m_3^{(i)})$, under the embedding $\mathrm{Sel}_2(E^i/K) \subset (K^\times/K^{\times 2})^3$ from Chapter 2.

Note that if we twist both D_a^1 and D_a^2 by $K(\sqrt{b})$ the resulting 2-coverings are D_{ab}^1 and D_{ab}^2. Hence if the twisted 2-coverings have solutions over K, then (9.1) will also have a solution over K.

The goal is then to find a quadratic twist, $b \in K^\times$, such that $D_{ab}^i \in \mathrm{Sel}_2(E_{ab}^i/K)$ and the essential 2-Selmer rank of E_{ab}^i is one, for $i = 1, 2$. Then if we assume that the Shafarevich-Tate group of both E_{ab}^i is finite, the Cassels-Tate pairing will be a perfect pairing of finite groups. Thus the 2-primary torsion of $Ш(E_{ab}^i)$ has square cardinality and is thus trivial. This implies that both D_{ab}^i are trivial in the Shafarevich-Tate group and hence have solutions over K.

Let $\mathcal{M}$ be the set of triples (m_1, m_2, m_3) such that each m_j is in the subgroup generated by the six elements $m_j^{(i)}$, $j = 1, 2, 3$ and $i = 1, 2$ in the group $K^\times/K^{\times 2}$.

We need to make the following assumptions:

1. E^1, E^2 have rational 2-torsion and distinct multiplicative places, $\mathfrak{p}_1, \mathfrak{p}_2$ respectively.

2. For each element m of $\mathcal{M}\backslash\{m^{(1)}, m^{(2)}, (1,1,1)\}$ there exists a $v \in S(E^1) \cup S(E^2)$ such that the 2-covering m is not locally solvable in K_v when viewed as a 2-covering of E^i for both $i = 1, 2$. Furthermore, for every $v \in S(E^1) \cup S(E^2)$ there exists an $a_v \in K_v$ such that both $D_{a_v}^1$ and $D_{a_v}^2$ are solvable in K_v.

3. $m^{(i)}$ is a unit at $\mathfrak{p}_i$, for $i = 1, 2$.

Remark 9.0.10. Assumptions 1 and 3 are weaker versions of Conditions Z_1, Z_2 from [Skorobogatov and Swinnerton-Dyer, 2005]. Assumption 2 is the same as Condition E of loc. cit.

Proposition 9.0.11. *[Skorobogatov and Swinnerton-Dyer, 2005, Corollary to Lemma 7] Suppose that (9.1) is everywhere locally soluble and that E^1, E^2 are both elliptic curves with K-rational 2-torsion. Furthermore, suppose that Assumption 2 holds. Then there exists an $a \in K^\times$ such that the 2-covering given by $m \in \mathcal{M}$ is everywhere locally soluble if and only if $m = m^{(1)}, m^{(2)}$ or $(1,1,1)$ for the elliptic curves E_a^i.*

The next proposition shows that if E^1, E^2 have distinct places of multiplicative reduction then the a from Proposition 9.0.11 can be chosen so that E_a^1, E_a^2 still have the same distinct places of multiplicative reduction and still satisfy the conclusion of that proposition. This proposition is a slight generalization of [Skorobogatov and Swinnerton-Dyer, 2005, Lemma 8].

Proposition 9.0.12. *Suppose that we are in the situation of Proposition 9.0.11 and a is chosen as in the proposition. If E^1, E^2 have distinct places of multiplicative reduction, $\mathfrak{p}_i$, then a can be chosen so that $\mathfrak{p}_i$ is a distinct place of multiplicative reduction of E^i_a. Furthermore E^i_a still satisfy the conclusions of Proposition 9.0.11.*

Proof. Let a be as in Proposition 9.0.11. The only way $\mathfrak{p}_i$ is not a distinct place of multiplicative reduction for E^i is if a is not a unit at $\mathfrak{p}_i$. Without loss of generality assume a is not a unit at $\mathfrak{p}_1$. Let $S \supseteq S(E^1_a) \cup S(E^2_a)$ be a finite set of places, $\mathfrak{p}$ be a prime such that $\mathfrak{p}/\mathfrak{p}_1 = (b)$ (modulo squares) and $b \in K_{\mathfrak{q}}^{\times 2}$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{p}_1\}$.

Since D^1_a is soluble at $\mathfrak{p}_1$ and $\mathfrak{p}_1$ is multiplicative, this implies that the triple $m^{(1)}$ is either in case 25 or 27 of [Skorobogatov and Swinnerton-Dyer, 2005, Lemma 4]. Then because $m^{(1)}$ is a unit at $\mathfrak{p}_1$, it must correspond to the triple $(1,1,1)$. Hence D^1_{ab} will be soluble at $\mathfrak{p}_1$ since $(1,1,1)$ is locally soluble regardless of the reduction type. Also, since b is a local square for the places in $S \setminus \{\mathfrak{p}_1\}$, the solubility of D^1_a implies the local solubility of D^1_{ab}. Similarly, the solubility of D^2_a implies that $m^{(2)}$ corresponds to a triple in case 25 of [Skorobogatov and Swinnerton-Dyer, 2005, Lemma 4]. Then because $m^{(2)}$ is a unit at $\mathfrak{p}_1$, it must correspond to the triple $(1,1,1)$. Hence D^2_{ab} will be soluble at $\mathfrak{p}_1$. Also, since b is a local square for the places in $S \setminus \{\mathfrak{p}_1\}$, the solubility of D^2_a implies the local solubility of D^2_{ab}. The Hilbert product formula applied to $(m^{(i)}_j, b)$ shows that $m^{(i)}_j$ is a square at $\mathfrak{p}$ and hence both D^1_{ab} and D^2_{ab} are soluble at $\mathfrak{p}$. Then ab satisfies the first part of the proposition.

Furthermore, by Proposition 9.0.11 any triple $m \in \mathcal{M}$ is not locally soluble (when viewed as a 2-covering of E^i_a) at some place $v \in S$. Also, $v \neq \mathfrak{p}_i$ since all the $m^{(i)}_j$ are locally squares at $\mathfrak{p}_1$ and thus any $m \in \mathcal{M}$ will also be a local square at $\mathfrak{p}_1$ (thus soluble at there). Then since the local solubility of m (when viewed as a 2-covering of E^i_a) away from $\mathfrak{p}_1$ is the same as the local solubility of m (when viewed as a 2-covering of E^i_{ab}) we get the desired statement. □

The next proposition shows that the conditions imposed above are not too strong, in that they can be related to the vanishing of the Brauer-Manin obstruction. Conjecturally the Brauer-Manin obstruction is the only obstruction to the Hasse Principle for K3 surfaces, and the next proposition provides a link between it and our assumptions.

Proposition 9.0.13. *[Skorobogatov and Swinnerton-Dyer, 2005, Theorem A.1] Suppose that we*

are in the situation of Proposition 9.0.12. If E^1, E^2 are not isogenous over $\bar{K}$ then the algebraic Brauer-Manin condition vanishes for the minimal projective desingularization of the surface (9.1).

Remark 9.0.14. Note that Assumption 1 implies that E^1 is not isogenous to E^2 over $\bar{K}$: Let v be a place of multiplicative reduction for E^1 and a place of good reduction for E^2, then the j-invariant of E^1 has negative valuation at v and the j-invariant of E^2 has non-negative valuation at v. Thus E^1, E^2 are not isogenous over $\bar{K}$.

Theorem 9.0.15. *If (9.1) is everywhere locally soluble, the three assumptions above hold and the relevant Shafarevich-Tate groups are finite then (9.1) has a solution in K, i.e. (9.1) satisfies the Hasse principle.*

Proof. The description at the beginning of this section shows how to take the locally soluble surface (9.1) and construct two 2-coverings (D^i), one for each E^i, $i = 1, 2$. By Assumption two and Proposition 9.0.12 there exists an a such that D^i_a is an element of $\mathrm{Sel}_2(E^i_a/K)$ for $i = 1, 2$ and the three assumptions above hold for E^i_a.

Assumption two implies that the hypotheses of Lemma 2.2.2 are satisfied, hence there exists a $b_1 \in K^\times$ such that both $E^i_{ab_1}$ have restricted 2-Selmer groups consisting of $D^i_{ab_1}$ and the identity element. Since b_1 is a unit at the bad places of E^1_a and E^2_a, the three assumptions above still hold for $E^i_{ab_1}$.

Assumptions one and three show that $E^i_{ab_1}$ satisfies the conditions of Corollary 8.0.9 (with the restricted 2-Selmer group described above), hence there exists a $b_2 \in K^\times$ such that both the elliptic curves $E^i_{ab_1b_2}$, for $i = 1, 2$, have essential 2-Selmer rank one (generated by $D^i_{ab_1b_2}$). Since b_2 is a unit at the bad places of $E^1_{ab_1}$ and $E^2_{ab_1}$, the three assumptions above still hold for $E^i_{ab_1b_2}$. Let $b = ab_1b_2$.

Hence $D^i_b \in \mathrm{Sel}_2(E^i_b/K)$ for $i = 1, 2$ and both E^i_b have essential 2-Selmer rank one. Then the assumption that the Shafarevich-Tate groups of E^i_b are both finite implies that the Cassels-Tate pairing is a perfect pairing of finite groups. Thus the 2-primary torsion of $Ш(E^i_b)$ has square cardinality and is thus trivial. This implies that both D^i_b actually come from the image of the Kummer map and hence have a solution over K. □

Part III

Bibliography

Bibliography

[Connell, 1993] Ian Connell. Good reduction of elliptic curves in abelian extensions. *J. Reine Angew. Math.*, 436:155–175, 1993.

[Cremona, 2001] J. E. Cremona. Classical invariants and 2-descent on elliptic curves. *J. Symbolic Comput.*, 31(1-2):71–87, 2001. Computational algebra and number theory (Milwaukee, WI, 1996).

[Dokchitser and Dokchitser, 2009] Tim Dokchitser and Vladimir Dokchitser. Elliptic curves with all quadratic twists of positive rank. *Acta Arith.*, 137(2):193–197, 2009.

[Dokchitser and Dokchitser, 2011] Tim Dokchitser and Vladimir Dokchitser. Root numbers and parity of ranks of elliptic curves. *J. Reine Angew. Math.*, 658:39–64, 2011.

[Heath-Brown, 1994] D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. II. *Invent. Math.*, 118(2):331–370, 1994. With an appendix by P. Monsky.

[Kobayashi, 2002] Shin-ichi Kobayashi. The local root number of elliptic curves with wild ramification. *Math. Ann.*, 323(3):609–623, 2002.

[Kolster, 2005] Manfred Kolster. The 2-part of the narrow class group of a quadratic number field. *Ann. Sci. Math. Québec*, 29(1):73–96, 2005.

[Kramer, 1981] Kenneth Kramer. Arithmetic of elliptic curves upon quadratic extension. *Trans. Amer. Math. Soc.*, 264(1):121–135, 1981.

[Mazur and Rubin, 2010] B. Mazur and K. Rubin. Ranks of twists of elliptic curves and Hilbert's tenth problem. *Invent. Math.*, 181(3):541–575, 2010.

[Monsky, 1996] P. Monsky. Generalizing the Birch-Stephens theorem. I. Modular curves. *Math. Z.*, 221(3):415–420, 1996.

[Rohrlich, 1996] David E. Rohrlich. Galois theory, elliptic curves, and root numbers. *Compositio Math.*, 100(3):311–349, 1996.

[Silverman, 1994] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Silverman, 2009] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Skinner and Urban, 2014] Christopher Skinner and Eric Urban. The Iwasawa main conjectures for GL_2. *Invent. Math.*, 195(1):1–277, 2014.

[Skinner, 2013] C. Skinner. A converse to a theorem of Gross, Zagier, and Kolyvagin. 2013. Preprint.

[Skorobogatov and Swinnerton-Dyer, 2005] Alexei Skorobogatov and Peter Swinnerton-Dyer. 2-descent on elliptic curves and rational points on certain Kummer surfaces. *Adv. Math.*, 198(2):448–483, 2005.

[Skorobogatov and Zarhin, 2008] Alexei N. Skorobogatov and Yuri G. Zarhin. A finiteness theorem for the Brauer group of abelian varieties and $K3$ surfaces. *J. Algebraic Geom.*, 17(3):481–502, 2008.

[Tian and Zhang, 2013] Yian X. Tian, Y. and S. Zhang. Genus Periods, Genus Points and Congruent Number Problem. 2013. Preprint.

[Zhang, 2013] W. Zhang. Selmer groups and divisibility of Heegner points. 2013. Preprint.