Received: 13 April 2023 | Accepted: 27 August 2023

DOI: 10.1112/blms.12931

SURVEY ARTICLE

Bulletin of the London Mathematical Society

Root numbers and parity phenomena

Lilybelle Cowland Kellock | **Vladimir Dokchitser**

University College London, London, UK

Correspondence
Lilybelle Cowland Kellock, University College London, London WC1H 0AY, UK.
Email: lilybelle.kellock.20@ucl.ac.uk

Funding information
Engineering and Physical Sciences Research Council, Grant/Award Number: EP/S021590/1; EPSRC Centre for Doctoral Training in Geometry and Number Theory (The London School of Geometry and Number Theory); University College London; Royal Society

Abstract

The parity conjecture has a long and distinguished history. It gives a way of predicting the existence of points of infinite order on elliptic curves without having to construct them, and is responsible for a wide range of unexplained arithmetic phenomena. It is one of the main consequences of the Birch and Swinnerton-Dyer conjecture and lets one calculate the parity of the rank of an elliptic curve using root numbers. In this handbook, we explain how to use local root numbers of elliptic curves to realise some of these phenomena, with an emphasis on explicit calculations. The text is aimed at a ‘user’ and, as such, we will not be concerned with the proofs of known cases of the parity conjecture, but instead, we will demonstrate the use of the theory by means of examples.

MSC 2020
11g05 (primary), 11g10, 11g40 (secondary)

Contents

1 | INTRODUCTION

1.1 | The parity conjecture

The Mordell–Weil rank of an elliptic curve E over a number field K remains mysterious. Calculating it is generally either hard or impossible, and there is currently no method that will provably work for every curve. All we have is ways of finding upper bounds by calculating the rank of Selmer groups, lower bounds by searching for K-rational points and fingers to cross that these coincide. In general, it can be hard to find out if an elliptic curve has even one K-rational point of infinite order.

The parity conjecture predicts points of infinite order and most known phenomena about elliptic curves effortlessly, after a simple calculation. It quantifies how the behaviour of E over completions of K should control the parity of the rank of E/K. It does this using the *global root number of* E/K, $w(E/K) \in \{\pm 1\}$, which is defined as the product of easily computable local factors at each place v of K, *local root numbers*. They are straightforward to compute since, despite having a non-constructive definition, they have been classified for all places (see §2).

Parity Conjecture. *Let E be an elliptic curve over a number field K. Then*

$$(-1)^{\mathrm{rk}(E/K)} = w(E/K),$$

where $w(E/K)$ is the global root number of E/K.

Note that if $w(E/K) = -1$, the parity conjecture implies that the rank is odd and, in particular, greater than 0. The parity conjecture is often the only way of predicting that a point of infinite order exists on an arbitrary elliptic curve. For now, take for granted that if E is a semistable elliptic curve defined over K, then

$$w(E/K) = (-1)^{m+u},$$

where m is the number of primes of K where E has split multiplicative reduction and u is the number of infinite places of K (see Corollary 2.5).

Example 1.1. Let us take

$$E : y^2 - 23y = x^3 - 99\,997x^2 - 17x + 42.$$

Magma [3] tells us that the rank of $E/\mathbb{Q}$ is 0, so that E does not have a rational point of infinite order. However, it also returns `false`, indicating that it has not proved that 0 is the rank of the curve.[†] With a simple calculation, the parity conjecture tells us that this curve should have a point of infinite order. Indeed, we have $\Delta_E = 17 \cdot 655\,943\,686\,625\,481\,101$ and non-split multiplicative reduction at both primes. Hence, since $\mathbb{Q}$ has one infinite place, the above result tells us that $w(E/\mathbb{Q}) = (-1)^1 = -1$, and so, the parity conjecture implies that the rank of $E/\mathbb{Q}$ is odd and that E has a point of infinite order.

One could use the conjecture of Birch and Swinnerton-Dyer to calculate Mordell–Weil ranks of elliptic curves. However, utilising the Birch–Swinnerton-Dyer conjecture requires computing L-functions, and, not only is this a rather lengthy calculation, we cannot provably compute $\mathrm{ord}_{s=1}L(E/\mathbb{Q}, s)$ unless it is 0, 1, 2 or 3, nor do we know the analytic continuation of L-functions of elliptic curves over general number fields. The beauty of the parity conjecture is that it is free of the conjectural machinery of L-functions and is an entirely arithmetical statement, yet it still allows us to predict the existence of points of infinite order.

In terms of applications, parity-related arguments have many notable consequences. For example, a known case of the p-parity conjecture[‡] was used by Bhargava and Shankar to prove that a positive proportion of elliptic curves over $\mathbb{Q}$ satisfies the Birch–Swinnerton-Dyer conjecture [1]. The parity conjecture settles most cases of the congruent number problem (see §3.12) and has been used to prove many results about the ranks of families of elliptic curves [15, 38, 54, 56]. A variant on the 2-parity conjecture was used to prove that Hilbert's Tenth Problem has a negative answer over rings of integers of number fields [47] and results on the parity of Selmer ranks were used to prove that certain Kummer surfaces satisfy the Hasse principle [64]. Similar arguments

[†] Of course, we could have done more extensive calculations; Magma only searches for points which have height below 15 and performs only 2- and 4-descent by default.

[‡] Namely that $\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/\mathbb{Q}) - \dim_{\mathbb{F}_p} E(\mathbb{Q})[p]$ is even if and only if $w(E/\mathbb{Q}) = +1$.

have also been used to prove results on class numbers of, for example, simplest cubic fields [72]. Root numbers also seem to have played a role in the early investigation of Heegner points and the Gross–Zagier formula, see, for example, [33] Chapter 5, Corollary 21.3, Conjecture 23.2 and [35].

The parity conjecture is easily deduced from the Birch–Swinnerton-Dyer conjecture together with the Hasse–Weil conjecture. The latter states that the completed L-function has analytic continuation to the whole of the complex plane and satisfies the functional equation $\hat{L}(E/K, s) = w(E/K)\hat{L}(E/K, 2-s)$, where $w(E/K)$ is the global root number. Assuming the Hasse–Weil conjecture, $w(E/K) = +1$ if and only if the completed L-function is symmetric around $s = 1$, which happens if and only if its order of vanishing at $s = 1$ is even. This tells us that

$$w(E/K) = (-1)^{\mathrm{ord}_{s=1}\hat{L}(E/K,s)},$$

which, assuming the Birch–Swinnerton-Dyer conjecture, gives the parity conjecture.

1.2 | A historical note

The investigation of parity-type questions appears to have begun with calculations of the parity of ranks of Selmer groups. In his 1954 paper, ‘A conjecture concerning rational points on cubic curves’ [60], Selmer gave an explicit definition of the first and second descent for $E/\mathbb{Q}$ with a rational 2-isogeny by writing out the equations they lead to. Selmer wrote that he had performed numerical calculations that suggest ‘when the first descent indicated at most three generators, then none or two of these seem to be excluded by the second descent’ (at most three as this was the case for all curves he numerically tested). Based on this, he conjectured that

1. *‘The second descent excludes an even number of generators’.*

In his 1962 paper ‘Arithmetic on curves of genus 1, III, The Tate Šafarevič and Selmer groups’ [5], where he coined the term ‘Selmer group’, Cassels extended Selmer’s conjecture and proved that the dimension of the image of $\mathrm{Sel}_{p^n}(E/K)$ under the map induced by multiplication by p^{n-1} differs from that of $\mathrm{Sel}_p(E/K)$, considered as a vector space over $\mathbb{F}_p$, by an even integer. This also treats the case of third descent, fourth descent, and so on. In [60], Selmer also conjectured the stronger statement, that

2. *‘The number of generators indicated by a first descent differs from the true number of generators by an even number’.*

Extending Selmer’s second conjecture to general p, as Cassels did for Selmer’s first conjecture, it says that the rank of the p-Selmer group determines the parity of the Mordell–Weil rank and is equivalent to saying that δ_p is even, where δ_p is the multiplicity of $\mathbb{Q}_p/\mathbb{Z}_p$ in $Ш(E/K)[p^\infty]$ and is conjecturally 0. In light of the parity conjecture and Selmer’s second conjecture, we would expect that

$$(-1)^{\mathrm{rk}_p(E/K)} = w(E/K),$$

where $\mathrm{rk}_p(E/K) = \mathrm{rk}(E/K) + \delta_p$ is the $\mathbb{Z}_p$-corank of the p-infinity Selmer group $\lim_{n\to\infty} \mathrm{Sel}_{p^n}(E/K)$. This is known as the *$p$-parity conjecture*. Although we will not discuss it or its applications in this handbook, tackling the p-parity conjecture has proved to be more fruitful than tackling the parity conjecture itself and there have been numerous works on the subject (see §1.3 for references). In this context, one can prove parity-related statements without assuming the finiteness of the Tate–Shafarevich group (the fabled Shafarevich–Tate conjecture), whereas the parity conjecture itself appears to be, as of now, unapproachable without this assumption.

1.3 | Using this handbook

This exposition is designed to explain how to calculate local and global root numbers of elliptic curves, and give a taste of what sorts of phenomena are predicted by the parity conjecture. The latter are concerned with the existence of rational points on elliptic curves for which there is as yet no construction, and that remain open problems without assuming the parity conjecture. As of now, the only known systematic construction of points of infinite order are Heegner points and self-points [13, 73], both using the modular parameterisation. We hope that our examples might inspire some new ideas for the construction of rational points.

In §2, we describe how to calculate local and global root numbers of elliptic curves, along with root numbers of quadratic twists of elliptic curves and twists of elliptic curves by self-dual Artin representations. We also give a first introduction as to how to use these to predict the existence of points of infinite order on elliptic curves. In §3, we illustrate how the parity conjecture predicts many unexplained arithmetic phenomena about rational points on elliptic curves. For a quick overview of these, see the table of contents. In §4, we propose an analogue of the minimalist conjecture for Artin twists of elliptic curves over $\mathbb{Q}$, and discuss its consequences. The conjecture gives the expected Galois module structure of $E(F) \otimes_{\mathbb{Z}} \mathbb{C}$, for a fixed Galois extension $F/\mathbb{Q}$ and a generic elliptic curve $E/\mathbb{Q}$.

The parity conjecture is known assuming the finiteness of the Tate–Shafarevich group [24, 48], and it is also known that these approaches to controlling the parity of the rank do not extend to controlling the Mordell–Weil rank modulo n for $n > 2$ [25]. We will not be concerned with approaches to the proof of the parity conjecture; for a self-contained exposition on the proof of the parity conjecture assuming the finiteness of the Tate–Shafarevich group (and of the proof of p-parity conjecture for elliptic curves over $\mathbb{Q}$), see [26]. We will confine ourselves to the setting of elliptic curves, although the parity conjecture is formulated for abelian varieties. For some recent results on these conjectures, see [7, 8, 19, 22–24, 28, 32, 41, 49–53]; for results on root numbers of abelian varieties, see [2, 58].

1.4 | Notation

We will use the following notation.

E	an elliptic curve
K	a number field
Δ_K	the discriminant of K
v	a place of K
K_v	the completion of K at a place v
$\langle \cdot, \cdot \rangle$	the usual inner product of (characters of) representations
Δ_E	the discriminant of a given Weierstrass equation for E

c_4, c_6	the usual invariants of an elliptic curve (see [63, p. 46])
N_E	the conductor of E
E_d	the quadratic twist of E by $d \in K^\times/K^{\times 2}$
$w(E/\mathcal{K})$	the local root number of E over a local field $\mathcal{K}$ (see §2.2)
$w(E/K)$	the global root number of E/K (see §2.1)
$w(E/K, \rho)$	the global root number of E/K twisted by an Artin representation ρ (see §2.4)

Most curves will be labelled with their Cremona label, if they have one.

2 | ROOT NUMBERS

2.1 | The global root number

Definition 2.1. Let E be an elliptic curve over a number field K. The *global root number* $w(E/K) \in \{\pm 1\}$ is defined as the product of *local root numbers* $w(E/K_v) \in \{\pm 1\}$,

$$w(E/K) = \prod_v w(E/K_v),$$

where the product runs over all places v of K, including infinite ones.

Local root numbers of elliptic curves are defined using epsilon factors of Weil–Deligne representations (see [14, 69] for the original definitions and [26] Section 3.3 for a more down-to-earth introduction). For a finite place v, the local root number is computed by looking at the action of the absolute Galois group of K_v on the ℓ-adic Tate module. For the purpose of this exposition, we will not concern ourselves with formal definitions, but will focus on how to calculate local root numbers in practice.

Remark 2.2. For an elliptic curve defined over $\mathbb{Q}$, the local root number at a prime p agrees with the eigenvalue of the associated Atkin–Lehner involution for the associated modular form. This follows from the corresponding statement for modular forms (see [59, Theorem 3.2.2], for example) together with the local Langlands conjecture for GL_2 and the modularity of elliptic curves over $\mathbb{Q}$.

2.2 | How to calculate local root numbers

Local root numbers of elliptic curves E/K have been classified for all places v of K, so, for most purposes, one can avoid the technical definitions.

Theorem 2.3. *Let E be an elliptic curve over a local field $\mathcal{K}$ of characteristic zero. When $\mathcal{K}$ is non-Archimedean, let k be its residue field and let $v : \mathcal{K}^\times \twoheadrightarrow \mathbb{Z}$ denote the normalised valuation with respect to $\mathcal{K}$. Let $(\frac{*}{k})$ denote the quadratic residue symbol on $k^\times$ and $(a, b)_{\mathcal{K}}$ denote the Hilbert symbol in $\mathcal{K}$.*

(i) *If $\mathcal{K}$ is Archimedean, then $w(E/\mathcal{K}) = -1$.*
(ii) *If $E/\mathcal{K}$ has good reduction, then $w(E/\mathcal{K}) = +1$.*

(iii) *If $E/\mathcal{K}$ has split multiplicative reduction, then $w(E/\mathcal{K}) = -1$.*

(iv) *If $E/\mathcal{K}$ has non-split multiplicative reduction, then $w(E/\mathcal{K}) = +1$.*

(v) *If $E/\mathcal{K}$ has additive, potentially multiplicative reduction and $\mathrm{char}(k) \geqslant 3$, then $w(E/\mathcal{K}) = (\frac{-1}{k})$.*

(vi) *If $E/\mathcal{K}$ has additive, potentially multiplicative reduction and $\mathrm{char}(k) = 2$, then $w(E/\mathcal{K}) = (-1, -c_6)_{\mathcal{K}}$. In particular, if $\mathcal{K} = \mathbb{Q}_2$, then*

$$w(E/\mathbb{Q}_2) = \begin{cases} -1 & \text{if } c_6' \equiv 1 \pmod 4; \\ +1 & \text{if } c_6' \equiv 3 \pmod 4, \end{cases}$$

where $c_6' = c_6/2^{v(c_6)}$.

(vii) *If $E/\mathcal{K}$ has additive, potentially good reduction and $\mathrm{char}(k) \geqslant 5$, then $w(E/\mathcal{K}) = (-1)^{\lfloor \frac{v(\Delta)|k|}{12} \rfloor}$, where Δ is the minimal discriminant of E.*

(viii) *If $E/\mathcal{K}$ has additive, potentially good reduction and $\mathrm{char}(k) \geqslant 3$, let $y^2 = x^3 + ax^2 + bx + c$ be a Weierstrass equation for E and let Δ_E be the discriminant of this model.*

- *If the Kodaira type*[†] *is* I_0^*, *then*

$$w(E/\mathcal{K}) = \left(\frac{-1}{k}\right).$$

- *If the Kodaira type is* III *or* III*, *then*

$$w(E/\mathcal{K}) = \left(\frac{-2}{k}\right).$$

- *If the Kodaira type is* II, IV, II* *or* IV*, *then there exists a Weierstrass equation for which $3 \nmid v(c)$. For such an equation, we have*

$$w(E/\mathcal{K}) = \delta \cdot (\Delta_E, c)_{\mathcal{K}} \cdot \left(\frac{v(c)}{k}\right)^{v(\Delta_E)} \cdot \left(\frac{-1}{k}\right)^{\frac{v(\Delta_E)(v(\Delta_E)-1)}{2}},$$

where $\delta \in \{\pm 1\}$ and $\delta = 1$ if and only if $\sqrt{\Delta_E} \in \mathcal{K}$.

The semistable case follows from the definitions in [14, 69], Rohrlich proved (*ii*)–(*vii*) in [55, §19] and [57, Theorem 2] (the case of $\mathcal{K} = \mathbb{Q}_2$ in (*vi*) can be found in [9, §3]), and (*viii*) is a result of Kobayashi [44, Theorem 1.1]. The statements of (*i*)–(*v*) and (*vii*), as they are written, are found in [24, Theorem 3.1]. For elliptic curves over local fields of positive characteristic, there is a similar classification of root numbers in [10, Theorem 3.1].

Theorem 2.3 does not tell us how to calculate local root numbers when E has additive potentially good reduction over a local field of residue characteristic 2. For $E/\mathbb{Q}_2$, one can use a classification of Halberstadt [36], which was extended to non-minimal Weierstrass models and potentially multiplicative reduction by Rizzo (see [54, Table III]). The tables that classify the local root number $w(E/\mathbb{Q}_2)$ can be found in the Appendix. Generalising Rizzo's and Halberstadt's tables to extensions of $\mathbb{Q}_2$ seems unfeasible as there would be many cases to check for large extensions. However, in the case of potentially good reduction over an extension of $\mathbb{Q}_2$, the local root number can be

[†] Recall that the Kodaira type of $E/\mathcal{K}$ can be calculated using Tate's algorithm (see [63, Ch. IV §9]).

described in terms of $\mathrm{Gal}(\mathcal{K}(E[3])/\mathcal{K}) \subset \mathrm{GL}(2, \mathbb{F}_3)$, see [20]. There is also a formula ([22, Theorem 1.12]) for local root numbers in terms of the Tamagawa number of E and the curves that are 2-isogenous to E over subfields of $\mathcal{K}(E[2])$; the Tamagawa numbers can be read off from Tate's algorithm [68] (or see [63, p. 365]).

Corollary 2.4. *Let E be an elliptic curve over a local field $\mathcal{K}$ of characteristic zero and residue characteristic $p \geqslant 5$. Let k denote the residue field of $\mathcal{K}$ and let $(\frac{*}{k})$ denote the quadratic residue symbol on k. Then*

$$w(E/\mathcal{K}) = \begin{cases} 1 & \textit{if } E/\mathcal{K} \textit{ has Kodaira type } \mathrm{I}_0; \\ \left(\frac{-1}{k}\right) & \textit{if } E/\mathcal{K} \textit{ has type } \mathrm{II}, \mathrm{II}^*, \mathrm{I}_n^* \textit{ or } \mathrm{I}_0^*; \\ \left(\frac{-2}{k}\right) & \textit{if } E/\mathcal{K} \textit{ has type } \mathrm{III} \textit{ or } \mathrm{III}^*; \\ \left(\frac{-3}{k}\right) & \textit{if } E/\mathcal{K} \textit{ has type } \mathrm{IV} \textit{ or } \mathrm{IV}^*; \\ -\left(\frac{6b}{k}\right) & \textit{if } E/\mathcal{K} \textit{ has type } \mathrm{I}_n, \end{cases}$$

where E is given by a Weierstrass equation $y^2 = x^3 + ax + b$, with $a, b \in \mathcal{O}_{\mathcal{K}}$.

Proof. For $\mathcal{K} = \mathbb{Q}_p$, this was proved in [56, Proposition 2]. If $E/\mathcal{K}$ has Kodaira type I_0, I_0^*, I_n^*, III or III*, these expressions follow immediately from the theorem. If $E/\mathcal{K}$ has type I_n, the root number depends on whether the reduction type is split or non-split. We may assume that the Weierstrass equation for E is minimal, since a change of model changes the value of b by a sixth power. Write

$$\bar{E} : y^2 = (x - \alpha)^2(x - \beta) \pmod{m_{\mathcal{K}}}$$

for the reduction of E modulo the maximal ideal of $\mathcal{K}$. $E/\mathcal{K}$ has split multiplicative reduction if and only if $\alpha - \beta \in k^{\times 2}$. Since $-\alpha^2\beta = b$ and $2\alpha + \beta = 0$ in k, we have

$$4\alpha^2(\alpha - \beta) = 4(\alpha^3 + b) = 4\left(-\frac{\alpha \cdot b}{\beta} + b\right) = 4\left(\frac{b}{2} + b\right) = 6b,$$

so that $(\frac{\alpha-\beta}{k}) = (\frac{6b}{k})$ and $w(E/\mathcal{K}) = -(\frac{6b}{k})$.

For the remaining cases of potentially good reduction, we show how the corollary follows from Theorem 2.3(*vii*). If $E/\mathcal{K}$ has type II, then $v(\Delta) = 2$ so

$$w(E/\mathcal{K}) = (-1)^{\left\lfloor \frac{|k|}{6} \right\rfloor} = \begin{cases} +1 & \text{if } |k| \equiv 1 \text{ or } 5 \pmod{12} \\ -1 & \text{if } |k| \equiv 7 \text{ or } 11 \pmod{12} \end{cases} = \left(\frac{-1}{k}\right).$$

A similar argument shows that if $E/\mathcal{K}$ has type II*, $w(E/\mathcal{K}) = (\frac{-1}{k})$. If $E/\mathcal{K}$ has type IV,

$$w(E/\mathcal{K}) = (-1)^{\left\lfloor \frac{|k|}{3} \right\rfloor} = \begin{cases} +1 & \text{if } |k| \equiv 1 \pmod{6} \\ -1 & \text{if } |k| \equiv 5 \pmod{6} \end{cases} = \left(\frac{-3}{k}\right),$$

and similarly, if E has type IV*, $w(E/\mathcal{K}) = (\frac{-3}{k})$, which completes the proof. □

Corollary 2.5. *Let E be a semistable elliptic curve defined over a number field K. Then*

$$w(E/K) = (-1)^{m+u},$$

where m is the number of primes of K where E has split multiplicative reduction and u is the number of infinite places of K.

Example 2.6. Let us take the curve

$$E : y^2 + y = x^3 - x^2. \quad (11A3)$$

This curve has split multiplicative reduction at 11 and good reduction everywhere else, so

$$w(E/\mathbb{Q}) = w(E/\mathbb{Q}_{11}) \cdot w(E/\mathbb{R}) = (-1)(-1) = +1.$$

Assuming the parity conjecture, this tells us that the rank of $E/\mathbb{Q}$ is even. In fact, E has rank 0 over $\mathbb{Q}$.

Example 2.7. Let us take the curve 11A3 as in the above example. We know that $w(E/\mathbb{Q}) = 1$. Let us look at what happens to the global root number of E over $K = \mathbb{Q}(\sqrt{-2})$. Since -2 is a quadratic residue modulo 11, 11 splits in K into, say, v and $\tilde{v}$. Then $w(E/K_v) = w(E/K_{\tilde{v}}) = -1$ since the reduction over K_v and $K_{\tilde{v}}$ is split multiplicative. Hence,

$$w(E/K) = w(E/K_v) \cdot w(E/K_{\tilde{v}}) \cdot w(E/\mathbb{C}) = (-1)^2 \cdot (-1) = -1.$$

Assuming the parity conjecture, this tells us that E must acquire a point of infinite order over K.

Asking what happens to local root numbers when we look at the curve over an extension of the base field will inform many of our examples of curious parity phenomena in §3. The above example illustrates the following key feature of root numbers of elliptic curves.

Lemma 2.8. *Let E/K be an elliptic curve and let F be a Galois extension of K. Let v be a prime of K and let v_1 and v_2 be primes above v in F. Then*

$$w(E/F_{v_1}) = w(E/F_{v_2}).$$

Proof. Since F/K is Galois, F_{v_1} is isomorphic to F_{v_2}. The isomorphism from F_{v_1} to F_{v_2} preserves the equation for E and the root number $w(E/F_{v_i})$ only depends on the isomorphism class of E/F_{v_i}. □

2.3 | Root numbers of quadratic twists of elliptic curves

If $E : y^2 = f(x)$ is an elliptic curve defined over a number field K and $d \in K^\times$, we call $E_d : dy^2 = f(x)$ the quadratic twist of E by d. Recall the following well-known relationship between the rank of E and the rank of E_d.

Lemma 2.9. *Let E be an elliptic curve defined over a number field K and let $d \in K^{\times} \setminus K^{\times 2}$. Then*

$$\mathrm{rk}(E/K(\sqrt{d})) = \mathrm{rk}(E/K) + \mathrm{rk}(E_d/K).$$

Lemma 2.10. *Let E/K and E_d/K be as above. Then*

$$w(E/K(\sqrt{d})) = w(E/K) \cdot w(E_d/K).$$

Remark 2.11. We caution the reader that the statement of Lemma 2.10 is not true on the level of local root numbers, see [7] Proposition 3.11 for the analogous statement in the local setting. The lemma follows from the local statement, along with the product formula for Hilbert symbols.

Lemma 2.10 tells us that the statement of the parity conjecture is consistent with what we know about the ranks of E and E_d. One can exploit this relationship between global root numbers and use the parity conjecture to predict the existence of points of infinite order on quadratic twists of elliptic curves.

Example 2.12. Let us take E to be the curve 11A3 over $\mathbb{Q}$ and let $K = \mathbb{Q}(\sqrt{-2})$. We saw in Examples 2.6 and 2.7 that $w(E/\mathbb{Q}) = +1$ and $w(E/K) = -1$. So, by Lemma 2.10, $w(E_{-2}/\mathbb{Q}) = -1$ and the parity conjecture implies that there is a rational point of infinite order on $E_{-2} : y^2 = x^3 - x^2 - x - 1$ over $\mathbb{Q}$. In fact, E_{-2} has rank 1 over $\mathbb{Q}$.

Theorem 2.13. *Let E be an elliptic curve over $\mathbb{Q}$.*

(i) *The function $d \mapsto w(E_d/\mathbb{Q})$ is periodic on the set of positive (resp. negative) square-free integers. The period divides $\prod_{p|N_E} p^2$ if N_E is odd and $4\prod_{p|N_E} p^2$ if N_E is even; in particular, it divides $4N_E^2$.*

(ii) *Root numbers of quadratic twists of E satisfy*

$$w(E_d/\mathbb{Q}) = \begin{cases} +1 \text{ for } 50\% \text{ of square-free } d; \\ -1 \text{ for } 50\% \text{ of square-free } d. \end{cases}$$

Proof. These results are well known, but we prove them here for lack of a reference.

(*i*) Let $D = \prod_{p|N_E} p^2$ if N_E is odd and $D = 4\prod_{p|N_E} p^2$ if N_E is even. Suppose $d_1 \equiv d_2 \pmod{D}$ and d_1 and d_2 have the same sign, and let $p \mid N_E$. First suppose $p > 2$. Since $d_1 \equiv d_2 \pmod{p^2}$ and d_1 and d_2 are square-free, it follows that $d_1/d_2 \equiv 1 \pmod{p}$, so d_1/d_2 is a square in $\mathbb{Q}_p$ by Hensel's lemma. So, $\mathbb{Q}_p(\sqrt{d_1}) = \mathbb{Q}_p(\sqrt{d_2})$ and for a prime $v \mid p$ in $\mathbb{Q}(\sqrt{d_1})$ and $\tilde{v}$ in $\mathbb{Q}(\sqrt{d_2})$, $w(E/\mathbb{Q}(\sqrt{d_1})_v) = w(E/\mathbb{Q}(\sqrt{d_2})_{\tilde{v}})$. Since p has the same splitting behaviour in $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$,

$$\prod_{v|p} w(E/\mathbb{Q}(\sqrt{d_1})_v) = \prod_{\tilde{v}|p} w(E/\mathbb{Q}(\sqrt{d_2})_{\tilde{v}}).$$

Now, if N_E is even and $p = 2$, $d_1 \equiv d_2 \pmod{16}$ and since d_1 and d_2 are square-free, it follows that $d_1/d_2 \equiv 1 \pmod{8}$ and d_1/d_2 is a square in $\mathbb{Q}_2$. Thus, $\prod_{v|2} w(E/\mathbb{Q}(\sqrt{d_1})_v) = \prod_{\tilde{v}|2} w(E/\mathbb{Q}(\sqrt{d_2})_{\tilde{v}})$ by the same argument as above. Finally, note that $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$ have the same number of infinite places. Hence,

$$w(E/\mathbb{Q}(\sqrt{d_1})) = (-1)^{v|\infty} \prod_{v|N_E} w(E/\mathbb{Q}(\sqrt{d_1})_v) = (-1)^{\tilde{v}|\infty} \prod_{\tilde{v}|N_E} w(E/\mathbb{Q}(\sqrt{d_2})_{\tilde{v}}) = w(E/\mathbb{Q}(\sqrt{d_2})).$$

Thus, $w(E_{d_1}/\mathbb{Q}) = w(E_{d_2}/\mathbb{Q})$ by Lemma 2.10.

(ii) First, we claim that we can find a $d_0 < 0$ such that $(d_0, 2N_E) = 1$ and, for every d, we have

$$w(E_{dd_0}/\mathbb{Q}) = -w(E_d/\mathbb{Q}).$$

Indeed, choose $d_0 < 0$ such that all the primes of bad reduction of E split in $\mathbb{Q}(\sqrt{d_0})$ and $(d_0, 2N_E) = 1$. By Lemma 2.8, this ensures that $w(E/\mathbb{Q}(\sqrt{d_0})) = -1$. If $d = d_0$, by Lemma 2.10,

$$w(E_{d_0^2}/\mathbb{Q}) = w(E/\mathbb{Q}) = w(E/\mathbb{Q}(\sqrt{d_0}))w(E_{d_0}/\mathbb{Q}) = -w(E_{d_0}/\mathbb{Q}).$$

If $d \neq d_0$, by Lemmas 2.10 and 2.8,

$$w(E/\mathbb{Q}) \cdot w(E_{d_0}/\mathbb{Q}) \cdot w(E_d/\mathbb{Q}) \cdot w(E_{dd_0}/\mathbb{Q}) = w(E/\mathbb{Q}(\sqrt{d}, \sqrt{d_0})) = +1$$

since $\mathbb{Q}(\sqrt{d}, \sqrt{d_0})$ has two infinite places and all finite places dividing the discriminant of E split into an even number of places in $\mathbb{Q}(\sqrt{d}, \sqrt{d_0})$. Now,

$$w(E/\mathbb{Q}) \cdot w(E_{d_0}/\mathbb{Q}) = w(E/\mathbb{Q}(\sqrt{d_0})) = -1.$$

Hence, $w(E_d/\mathbb{Q}) \cdot w(E_{dd_0}/\mathbb{Q}) = -1$ and we have proved the claim.

Now, to finish proving the theorem, take d_0 as above and D as in the proof of (i). By part (i) of the theorem, the function $d \mapsto w(E_d/\mathbb{Q})$ is periodic on the set of positive (resp. negative) square-free integers with the period dividing D. The involution $d \leftrightarrow d \cdot d_0$ changes the sign of the root number that is, for any d such that $w(E_d/\mathbb{Q}) = +1$, we have $w(E_{d \cdot d_0}/\mathbb{Q}) = -1$. Since d_0 is coprime to D, the density of square-free integers congruent to d modulo D is the same as the density of those congruent to dd_0 modulo D, see, for example, [39]. The result follows. □

Theorem 2.13 gives a heuristic for Goldfeld's conjecture, which states that there is a 50/50 distribution of the rank being 0 and 1 in a quadratic twist family over $\mathbb{Q}$, see [31, Conjecture B]. Over general number fields, root numbers of quadratic twists are also periodic (by essentially the same proof). However, the distribution of the root numbers can be different. As an extreme case, it is possible for all quadratic twists to have the same root number; see §3.9 or [21] for the original discussion. In [42, Example 7.11] and [43], it is shown that the set of proportions that appear for elliptic curves is dense in [0,1]. In [42] and [43], this is phrased in terms of 2-Selmer ranks — this is equivalent to the corresponding statement for global root numbers because the 2-parity conjecture is known in this instance by [23, Theorem 1.3].

Remark 2.14. We expect that for elliptic curves over $\mathbb{Q}$ in a suitable ordering, there is a 50/50 distribution of the global root number being +1 and −1 (for the ordering used, see Notation 4.2). Despite the fact that this is a statement about root numbers rather than about ranks, this remains an open problem.

2.4 | Root numbers of Artin twists of elliptic curves

Let E/K be an elliptic curve and let F be a Galois extension of K. Then $E(F) \otimes_{\mathbb{Z}} \mathbb{C}$ is naturally a $\mathrm{Gal}(F/K)$-representation by letting elements of the Galois group act on the co-ordinates of the F-rational points of E. There is a parity conjecture for Artin twists of elliptic curves which describes the parity of the multiplicity of an irreducible, self-dual $\mathrm{Gal}(F/K)$-representation ρ in $E(F) \otimes_{\mathbb{Z}} \mathbb{C}$. Since $\mathrm{rk}(E/F) = \dim E(F) \otimes_{\mathbb{Z}} \mathbb{C}$, this can tell us about the existence of rational points over F. The parity conjecture for twists is especially striking when the usual parity conjecture does not provide us with any information about the existence of rational points (see Example 2.19). We state the parity conjecture for Artin twists here and present a theorem that allows us to explicitly calculate global root number of twists of elliptic curves over $\mathbb{Q}$ by self-dual Artin representations when the conductor of ρ is coprime to the conductor of E.

Parity Conjecture for Twists. *Let E/K be an elliptic curve over a number field and let ρ be a self-dual Artin representation of $\mathrm{Gal}(\bar{K}/K)$ that factors through $\mathrm{Gal}(F/K)$, for a finite extension F/K. Then*

$$(-1)^{\langle \rho, E(F) \otimes_{\mathbb{Z}} \mathbb{C} \rangle} = w(E/K, \rho),$$

where $w(E/K, \rho)$ is the global root number of the twist of E by ρ.

Theorem 2.15 [27, Corollary 2]. *Let ρ be a self-dual Artin representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Let E be an elliptic curve over $\mathbb{Q}$ whose conductor N_E is coprime to the conductor of ρ. Then*

$$w(E/\mathbb{Q}, \rho) = w(E/\mathbb{Q})^{\dim \rho} \cdot \mathrm{sign}(\alpha_\rho) \cdot \left(\frac{\alpha_\rho}{N_E}\right),$$

where $(\frac{*}{*})$ is the Jacobi symbol and $\alpha_\rho = 1$ if $\det(\rho) = \mathbb{1}$ and, otherwise, α_ρ is such that the character $\det(\rho)$ factors through $\mathbb{Q}(\sqrt{\alpha_\rho})$. We adopt the convention that $(\frac{\alpha_\rho}{2}) = -1$ if $\alpha_\rho \equiv 5 \pmod 8$ and $(\frac{\alpha_\rho}{2}) = +1$ if $\alpha_\rho \equiv 1 \pmod 8$.

Note that if $2 \mid N_E$, then 2 does not ramify in $\mathbb{Q}(\sqrt{\alpha_\rho})$ since we assumed the conductor of ρ to be coprime to the conductor of E, and hence $\alpha_\rho \equiv 1$ or $5 \pmod 8$. For a statement that allows multiplicative reduction at primes dividing the conductor of ρ, see [27, Theorem 1]. Local root numbers of Artin twists of elliptic curves have been classified by Rohrlich (with restrictions in residue characteristic 2 and 3), see [57, Theorem 2].

We present the following important properties of global root numbers of twists, which are also of use when predicting the existence of rational points of infinite order using the parity conjecture for twists (see Example 2.19). For reference, (i) and (ii) follow from the definition of local root numbers (see [14] for more details) and (iii) and (iv) can be found in [23, Proposition A.2].

Theorem 2.16. *Let E be an elliptic curve over a number field K. Let ρ and ρ' be Artin representations of $G_K = \mathrm{Gal}(\bar{K}/K)$. Let L/K be a finite extension and let τ be an Artin representation of $G_L = \mathrm{Gal}(\bar{L}/L)$. Then*

(i) $w(E/K, \mathbb{1}) = w(E/K)$;
(ii) $w(E/K, \rho \oplus \rho') = w(E/K, \rho) \cdot w(E/K, \rho')$;

(iii) $w(E/K, \mathrm{Ind}_{G_L}^{G_K} \tau) = w(E/L, \tau)$ *and, in particular,* $w(E/L) = w(E/K, \mathrm{Ind}_{G_L}^{G_K} \mathbb{1})$*;*
(iv) $w(E/K, \rho \oplus \rho^*) = +1$*, where* ρ^* *is the dual representation.*

We can relate the rank over subfields of F to the representation $E(F) \otimes_{\mathbb{Z}} \mathbb{C}$ using the following lemma.

Lemma 2.17. *Let* E *be an elliptic curve over* K *and let* F *be a Galois extension with* $G = \mathrm{Gal}(F/K)$*. Then for every* $H \leqslant G$*,*

$$\mathrm{rk}(E/F^H) = \langle \mathbb{C}[G/H], E(F) \otimes_{\mathbb{Z}} \mathbb{C} \rangle_G.$$

Proof. For a subgroup $H \leqslant G$, we have $\mathrm{rk}(E/F^H) = \dim(E(F) \otimes_{\mathbb{Z}} \mathbb{C})^H$ and

$$\dim(E(F) \otimes_{\mathbb{Z}} \mathbb{C})^H = \langle \mathbb{1}, \mathrm{Res}_H^G E(F) \otimes_{\mathbb{Z}} \mathbb{C} \rangle_H \overset{(1)}{=} \langle \mathrm{Ind}_H^G \mathbb{1}, E(F) \otimes_{\mathbb{Z}} \mathbb{C} \rangle_G = \langle \mathbb{C}[G/H], E(F) \otimes_{\mathbb{Z}} \mathbb{C} \rangle_G,$$

where (1) follows from Frobenius reciprocity. □

The following lemma tells us that in many cases (for instance symmetric groups), the parity conjecture for twists follows from the usual parity conjecture.

Lemma 2.18. *Let* E/K *be an elliptic curve and let* F/K *be a Galois extension of number fields. Let* ρ *be a representation of* $G = \mathrm{Gal}(F/K)$ *that can be written as a linear combination of permutation modules, that is,*

$$\rho \oplus \bigoplus_i \mathrm{Ind}_{H_i}^G \mathbb{1} \simeq \bigoplus_j \mathrm{Ind}_{H'_j}^G \mathbb{1}$$

for some H_i*,* $H'_j \leqslant G$*. If the parity conjecture holds for* E *over* $L_i = F^{H_i}$ *for all* i *and* $L'_j = F^{H'_j}$ *for all* j*, then the twisted parity conjecture holds for* E *and* ρ*.*

Proof. By Theorem 2.16 and assuming the usual parity conjecture for L_i and L_j,

$$w(E/K, \rho) = \frac{\prod_j w(E/K, \mathrm{Ind}_{H'_j}^G \mathbb{1})}{\prod_i w(E/K, \mathrm{Ind}_{H_i}^G \mathbb{1})} = \frac{\prod_j w(E/L_j)}{\prod_i w(E/L_i)} = (-1)^{\sum_j \mathrm{rk}(E/L_j) - \sum_i \mathrm{rk}(E/L_i)}.$$

By Lemma 2.17,

$$\sum_j \mathrm{rk}(E/L_j) - \sum_i \mathrm{rk}(E/L_i) = \sum_j \langle E(F) \otimes_{\mathbb{Z}} \mathbb{C}, \mathrm{Ind}_{H'_j}^G \mathbb{1} \rangle - \sum_i \langle E(F) \otimes_{\mathbb{Z}} \mathbb{C}, \mathrm{Ind}_{H_i}^G \mathbb{1} \rangle$$
$$= \langle E(F) \otimes_{\mathbb{Z}} \mathbb{C}, \rho \rangle.$$

Thus, the parity conjecture for twists holds for E and ρ. □

When the condition of Lemma 2.18 is not satisfied, the parity conjecture for twists gives us more information about the arithmetic of elliptic curves than the usual parity conjecture, as we now illustrate.

Example 2.19. Let us take the elliptic curve of rank 1 over $\mathbb{Q}$

$$E : y^2 + y = x^3 - x. \quad (37A1)$$

Let F be the splitting field of the polynomial

$$x^{10} - x^9 + 6x^8 - 3x^7 + 11x^6 - 3x^5 + 11x^4 - 3x^3 + 6x^2 - x + 1,$$

which has discriminant -47^5. Then $G = \mathrm{Gal}(F/\mathbb{Q}) = D_{10}$, the dihedral group with 10 elements. We can predict the existence of points of infinite order on E/F using the parity conjecture for twists as follows.

The subgroups of D_{10}, up to conjugacy, are the trivial group, C_2, C_5 and D_{10}. The irreducible representations of D_{10} are the trivial representation $\mathbb{1}$, sign representation ϵ and two 2-dimensional representations ρ_1 and ρ_2. Now let $V = E(F) \otimes_{\mathbb{Z}} \mathbb{C}$. This is a G-representation, so we can decompose it as

$$V = \mathbb{1}^{\oplus a} \oplus \epsilon^{\oplus b} \oplus \rho_1^{\oplus c} \oplus \rho_2^{\oplus d}.$$

Since the character of this representation is rational, ρ_1 and ρ_2 must appear with the same multiplicity as their characters are $G_{\mathbb{Q}}$-conjugate. So, we have $V = \mathbb{1}^{\oplus a} \oplus \epsilon^{\oplus b} \oplus \rho_1^{\oplus c} \oplus \rho_2^{\oplus c}$. By Lemma 2.17, for any subgroup $H \leqslant \mathrm{Gal}(F/\mathbb{Q})$,

$$\mathrm{rk}(E/F^H) = \dim V^H = \langle \mathbb{C}[G/H], V\rangle_G.$$

Observe that

$$\mathbb{C}[D_{10}/D_{10}] = \mathbb{1}, \qquad \mathbb{C}[D_{10}/C_5] = \mathbb{1} \oplus \epsilon, \qquad \mathbb{C}[D_{10}/C_2] = \mathbb{1} \oplus \rho_1 \oplus \rho_2,$$
$$\mathbb{C}[D_{10}] = \mathbb{1} \oplus \epsilon \oplus \rho_1^{\oplus 2} \oplus \rho_2^{\oplus 2}.$$

Hence,

$$\mathrm{rk}(E/F^H) = \begin{cases} a & \text{when } H = D_{10}; \\ a + b & \text{when } H = C_5; \\ a + 2c & \text{when } H = C_2; \\ a + b + 4c & \text{when } H = \{1\}. \end{cases}$$

E has non-split multiplicative reduction at 37 and good reduction everywhere else. Since 37 splits in $F^{C_5} = \mathbb{Q}(\sqrt{-47})$, by Corollary 2.5, we find that

$$w(E/\mathbb{Q}) = -1 \quad \text{and} \quad w(E/\mathbb{Q}(\sqrt{-47})) = -1.$$

So, the parity conjecture and our calculations above imply that the rank of E is odd over all four intermediate fields. In particular, we could, in principle, have $\mathrm{rk}(E/F) = \mathrm{rk}(E/\mathbb{Q})$.

We now use the parity conjecture for twists to show that c is odd, and hence $\mathrm{rk}(E/F) \geqslant \mathrm{rk}(E/\mathbb{Q}) + 4 \geqslant 5$. Using the notation of Theorem 2.15, we have $N_E = 37$ and $\alpha_{\rho_1} = -47$ since

$\det(\rho_1) = \epsilon$. Hence, by Theorem 2.15,

$$w(E/\mathbb{Q}, \rho_1) = (-1)^2 \cdot (-1) \cdot \left(\frac{-47}{37}\right) = -1.$$

Thus, since $\langle \rho_1, E(F) \otimes_{\mathbb{Z}} \mathbb{C} \rangle = c$, the parity conjecture for twists tells us that c must be odd and hence $\mathrm{rk}(E/F) \geqslant 5$. In fact, assuming the parity conjecture for twists, the rank of E/F is larger than the rank of E over any of the subfields.

3 | PARITY PHENOMENA

We now turn to examples of phenomena that are predicted by the parity conjecture as a result of root number calculations. Subsections 3.6 and 3.14–3.17 deal with consequences of the parity conjecture for Artin twists. We stress that all 'parity phenomena' that we describe, including the statements in all of the subsection titles, are conditional on the parity conjecture and are effectively unsolved problems. Most of these have been observed before; only §3.8, §3.14 and §3.15 are new. The titles are designed to give specific examples of what will be discussed; the general statements will be contained within the subsections. The subsections are largely independent of one another and can be read in almost any order.

3.1 | Every $E/\mathbb{Q}$ has even rank over $\mathbb{Q}(\sqrt{-3}, \sqrt{13})$

Example 3.1 (See also [26], Conjecture 8.7). The parity conjecture predicts that every elliptic curve $E/\mathbb{Q}$ has even rank over $K = \mathbb{Q}(\sqrt{-3}, \sqrt{13})$. To see this, we note that every rational prime splits into an even number of primes in K. Indeed, the decomposition group of rational primes away from the discriminant of K is cyclic and so cannot be isomorphic to $C_2 \times C_2$. Hence, these primes split into two or four primes in K. The primes that divide the discriminant of K are 3 and 13, and we note that 3 splits in $\mathbb{Q}(\sqrt{13})$ and 13 splits in $\mathbb{Q}(\sqrt{-3})$. So, 3 and 13 each split into two primes in K. Thus,

$$\begin{aligned} w(E/K) &= \prod_{v|\infty} w(E/K_v) \cdot \prod_{v|N_E} w(E/K_v) = w(E/\mathbb{C})^2 \cdot \prod_{p|N_E} \prod_{v|p} w(E/K_v) = (-1)^2 \cdot \prod_{p|N_E} (\pm 1)^{2 \text{ or } 4} \\ &= +1, \end{aligned}$$

where v runs over primes of K and p runs over primes of $\mathbb{Q}$. Here, we have used the fact that if v and v' lie above the same prime p, then $w(E/K_v) = w(E/K_{v'})$ by Lemma 2.8. Assuming the parity conjecture, we deduce that E has even rank over K.

The same reasoning gives us the following lemma.

Lemma 3.2. *Let E/K be an elliptic curve and let F be a finite Galois extension of K in which every place of K splits into an even number of places. Then, assuming the parity conjecture, E has even rank over F.*

Example 3.3. Let

$$E : y^2 + xy = x^3 - x^2 + 4x - 3. \quad (73A1)$$

Since E has split multiplicative reduction at 73, Corollary 2.5 tells us that $w(E/\mathbb{Q}) = +1$. This curve has a fairly obvious point over $K = \mathbb{Q}(\sqrt{-3}, \sqrt{13})$, namely $(0, \sqrt{-3})$, which turns out to have infinite order. Example 3.1 tells us that $\mathrm{rk}(E/K)$ is even, so there should be another (independent) point of infinite order over K. In effect, the existence of a point of infinite order over $\mathbb{Q}(\sqrt{-3})$ forces the existence of another point of infinite order over $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{13})$ or $\mathbb{Q}(\sqrt{-39})$. In this case, local root number calculations show that $w(E/\mathbb{Q}(\sqrt{13})) = -1$, so, assuming the parity conjecture, there should also be a K-rational point of infinite order coming from points on E over $\mathbb{Q}(\sqrt{13})$. Indeed, the point $(3, -\frac{3\sqrt{13}+3}{2})$ lies on E and generates the infinite part of the Mordell–Weil group of $E/\mathbb{Q}(\sqrt{13})$. It is not at all clear how the points over $\mathbb{Q}(\sqrt{13})$ relate to those over $\mathbb{Q}(\sqrt{-3})$, and why the existence in one of the fields guarantees the existence in the other.

3.2 | Every $E/\mathbb{Q}$ has even rank over any $C_2 \times C_2 \times C_2 \times C_2$ extension of $\mathbb{Q}$

Lemma 3.2 also gives us the following example.

Example 3.4. Let K be any Galois extension of $\mathbb{Q}$ with Galois group C_2^d, where $d \geqslant 4$ and let E be an elliptic curve defined over $\mathbb{Q}$. We claim that E should have even rank over K. As in Example 3.1, all unramified primes split into an even number of primes in K. We claim that every ramified prime splits into an even number of primes in K, too. If $p > 2$, note that the largest extension of $\mathbb{Q}_p$ we can get when we localise at a prime v above p in K has Galois group $C_2 \times C_2$ since $\mathbb{Q}_p^{\times}/\mathbb{Q}_p^{\times 2} \cong C_2 \times C_2$ for $p > 2$. Hence, the decomposition group of $v \mid p$ has size at most 4, and so, there must be at least four primes above p in K. Similarly, for $p = 2$, the largest extension of $\mathbb{Q}_2$ we can get when we localise at a prime v above 2 has Galois group $C_2 \times C_2 \times C_2$, and so, the decomposition group of $v \mid 2$ has size at most 8 and there are at least two primes above 2 in K. Since K has an even number of infinite places, Lemma 3.2 tells us that, assuming the parity conjecture, E has even rank over K.

Remark 3.5. The parity conjecture implies that if $E/\mathbb{Q}$ has a point of infinite order over a $C_2 \times C_2 \times C_2 \times C_2$-extension of $\mathbb{Q}$, it must automatically acquire a second one. This suggests that over any $C_2 \times C_2 \times C_2 \times C_2$-extension of $\mathbb{Q}$, there might be some as yet unknown extra symmetry, for instance, in the Mordell–Weil group, which would explain why the rank is even. As Example 3.3 illustrates, it is not clear what such a symmetry might be.

3.3 | $y^2 + xy = x^3 + Ax + B$ where $A \equiv B \pmod{2}$ has infinitely many solutions over $\mathbb{Q}(\zeta_8)$

Example 3.6. The parity conjecture predicts that every elliptic curve $E/\mathbb{Q}$ with split multiplicative reduction at 2 has infinitely many rational points over $K = \mathbb{Q}(\zeta_8)$. Here, the only ramified prime is 2, which is totally ramified. So, if E has split multiplicative reduction at 2, for the unique prime v above 2 in K, we have $w(E/K_v) = -1$ by Theorem 2.3. Note that $\mathrm{Gal}(K/\mathbb{Q}) \cong C_2 \times C_2$, so in the same vein as Example 3.1, all primes away from 2 split into an even number of primes in K, which means that their product contributes a $+1$ to the root number. There are two infinite places, and so, these also contribute a $+1$ to the root number. Hence, $w(E/K) = -1$ and the parity conjecture predicts that E has odd rank over K. In particular, it says that E has infinitely many $\mathbb{Q}(\zeta_8)$-rational points. We emphasise that it is not at all clear how to construct these points!

The above working tells us that every elliptic curve over $\mathbb{Q}$ of the form $E : y^2 + xy = x^3 + Ax + B$, where $A \equiv B \pmod 2$, has infinitely many points over $\mathbb{Q}(\zeta_8)$ since every such curve has split multiplicative reduction at 2. The example easily generalises to the following statement.

Lemma 3.7. *Suppose that $K/\mathbb{Q}$ is a biquadratic extension and that exactly one prime p does not split in $K/\mathbb{Q}$. If the parity conjecture holds, then every elliptic curve $E/\mathbb{Q}$ with split multiplicative reduction at p has a point of infinite order over K.*

Example 3.8. The curves

(i) $E : y^2 + xy = x^3 - 3x + 1$ (34A1),
(ii) $E' : y^2 + xy = x^3 - 34x + 68$ (102B1) and
(iii) $E'' : y^2 + xy = x^3 - 2x - 2$ (922A1).

each have split multiplicative reduction at 2, so by Example 3.6, the parity conjecture implies that these curves all have infinitely many points over $\mathbb{Q}(\zeta_8)$. In fact, all of these curves have global root number $+1$ over $\mathbb{Q}$, so the rank must grow in $\mathbb{Q}(\zeta_8)$. One can perform descent calculations to show that the rank of each of these curves over $\mathbb{Q}(\zeta_8)$ is 1. However, the point comes from a different quadratic subfield for each curve: E has a point of infinite order over $\mathbb{Q}(\sqrt{2})$, E' has a point of infinite order over $\mathbb{Q}(\sqrt{-1})$ and E'' has a point of infinite order over $\mathbb{Q}(\sqrt{-2})$.

Remark 3.9 (See also [25], Remark 4). Consider the elliptic curve $E : y^2 = x^3 + x^2 - x$, which has Kodaira type IV over $\mathbb{Q}_2$. By computing root numbers of the quadratic twists of E by -1, 2 and -2 and using Lemma 2.10, we find that $w(E/\mathbb{Q}(\zeta_8)) = -1$. The parity conjecture predicts that E has odd rank over $\mathbb{Q}(\zeta_8)$ in a similar way to Example 3.6. The fact that $E/\mathbb{Q}(\zeta_8)$ has odd analytic rank has the following consequence for L-functions.

Since all primes away from 2 split in $\mathbb{Q}(\zeta_8)$ and E has additive reduction at the prime above 2 in $\mathbb{Q}(\zeta_8)$, the Euler product of the L-function of $E/\mathbb{Q}(\zeta_8)$ is formally a square, in the sense that each Euler factor appears an even number of times:

$$L(E/\mathbb{Q}(\zeta_8), s) = 1 \cdot \frac{1}{(1 + 2 \cdot 9^{-s} + 9^{1-2s})^2} \frac{1}{(1 + 25^{-s})^2} \frac{1}{(1 + 10 \cdot 49^{-s} + 49^{1-2s})^2} \cdots .$$

If we define $F(s)$ by the square root of this Euler product so that $F(s)^2 = L(E/\mathbb{Q}(\zeta_8), s)$ for $\mathrm{Re}(s) > \frac{3}{2}$, then $F(s)$ shares many properties that one would expect from an L-function. However, it does not have analytic continuation to $s = 1$ since the order of vanishing of $L(E/\mathbb{Q}(\zeta_8), s)$ at $s = 1$ is odd.

3.4 | $y^2 + y = x^3 + x^2 + x$ has infinitely many $\mathbb{Q}(\sqrt[3]{m})$-rational solutions for every m

Example 3.10 (As considered in [27]). The elliptic curve

$$E : y^2 + y = x^3 + x^2 + x \quad (19\mathrm{A}3)$$

has rank 0 over $\mathbb{Q}$. We claim that, assuming the parity conjecture, it has infinitely many $\mathbb{Q}(\sqrt[3]{m})$-rational solutions for every cube-free $m > 1$. First, note that $\Delta_E = 19$, and E has split multiplicative reduction at 19. Hence, $w(E/K_v) = -1$ at primes v above 19. So, to calculate the global root number, all we need to know is how many primes there are above 19 in $\mathbb{Q}(\sqrt[3]{m})$. If $19 \nmid m$, the Kummer–Dedekind theorem tells us that there is either one or three primes above 19, corresponding to whether $X^3 - m$ is irreducible or splits completely over $\mathbb{F}_{19}$. If $19 \mid m$, it is totally ramified. The product of local root numbers at the infinite places is $+1$ since $\mathbb{Q}(\sqrt[3]{m})$ has one real embedding and one complex embedding. This tells us that

$$w(E/\mathbb{Q}(\sqrt[3]{m})) = (-1)^{1 \text{ or } 3} = -1.$$

So, assuming the parity conjecture, E must have infinitely many $\mathbb{Q}(\sqrt[3]{m})$-rational points.

We can numerically compute the points of infinite order on E over $\mathbb{Q}(\sqrt[3]{m})$ for small m (for $m = 1, \dots, 7$, E has rank 1 over $\mathbb{Q}(\sqrt[3]{m})$).

$\boldsymbol{m}$	**Generator of** $\boldsymbol{E(\mathbb{Q}(\sqrt[3]{m}))/E(\mathbb{Q}(\sqrt[3]{m}))_{\mathrm{tors}}}$
2	$(2\sqrt[3]{2}^2 - \sqrt[3]{2},\quad -2\sqrt[3]{2}^2 + \sqrt[3]{2} + 5)$
3	$(\frac{13\sqrt[3]{3}^2+6\sqrt[3]{3}-3}{25},\quad \frac{-52\sqrt[3]{3}^2-24\sqrt[3]{3}-213}{125})$
4	$(\frac{-\sqrt[3]{4}^2+4\sqrt[3]{4}}{2},\quad \frac{\sqrt[3]{4}^2-4\sqrt[3]{4}+10}{2})$
5	$(\frac{82\sqrt[3]{5}^2-144\sqrt[3]{5}-160}{529},\quad \frac{-574\sqrt[3]{5}^2+1008\sqrt[3]{5}-6815}{12\,167})$
6	$(\frac{7340\sqrt[3]{6}^2-8885\sqrt[3]{6}-9450}{90\,774},\quad \frac{748\,680\sqrt[3]{6}^2-906\,270\sqrt[3]{6}-992\,477}{11\,165\,202})$
7	$(\frac{50\sqrt[3]{7}^2-40\sqrt[3]{7}}{63},\quad \frac{-150\sqrt[3]{7}^2+120\sqrt[3]{7}+811}{189})$

Without the parity conjecture, proving the existence of these points for all m seems completely out of reach. In [18], it is shown that for an elliptic curve E over a number field K, the rank of E goes up in infinitely many extensions of K obtained by adjoining a cube root of an element of K. However, these points account for very few m in Example 3.10.

Remark 3.11. We caution the reader that in the above example there are no parametric solutions of the form

$$f : m \mapsto P_m \in E(\mathbb{Q}(\sqrt[3]{m})).$$

Indeed, if f were analytic, it would give an analytic map $\mathbb{P}^1 \to E(\mathbb{C})$ which contradicts the Riemann–Hurwitz formula. If f were only assumed to be continuous, it would give a map $\mathbb{R} \to E(\mathbb{R})$. For $m \in \mathbb{Q}^{\times 3}$, this could only take values (0,0), (0,1) or $\mathcal{O}$, which would force f to be constant.

3.5 | $E : y^2 + y = x^3 + x^2 + x$ has rank at least n over $\mathbb{Q}(\sqrt[3^n]{m})$

Example 3.12. Example 3.10 tells us that the rank of $E : y^2 + y = x^3 + x^2 + x$ (19A3) must grow over $\mathbb{Q}(\sqrt[3]{m})$. Assuming the parity conjecture, it grows at every step of the tower $(\mathbb{Q}(\sqrt[3^n]{m}))_{n \geqslant 1}$. To see this, we claim that 19 splits into an odd number of places in $\mathbb{Q}(\sqrt[3^n]{m})$. Indeed, $\mathbb{Q}_{19}(\zeta_{3^n}, \sqrt[3^n]{m})$ is an odd degree extension of $\mathbb{Q}_{19}$ and so $e_{\tilde{v}} f_{\tilde{v}}$ is odd for every prime $\tilde{v}$ above 19 in $\mathbb{Q}(\zeta_{3^n}, \sqrt[3^n]{m})$, where $e_{\tilde{v}}$ is the ramification degree and $f_{\tilde{v}}$ is the residue degree of $\tilde{v}$ over 19. Let v be a prime above 19 in $\mathbb{Q}(\sqrt[3^n]{m})$. Since $e_v f_v$ divides $e_{\tilde{v}} f_{\tilde{v}}$, $e_v f_v$ is also odd. Then, since $[\mathbb{Q}(\sqrt[3^n]{m}) : \mathbb{Q}]$ is odd and $[\mathbb{Q}(\sqrt[3^n]{m}) : \mathbb{Q}] = \sum_{i=1}^{k} e_{v_i} f_{v_i}$, the sum over all primes above 19 in $\mathbb{Q}(\sqrt[3^n]{m})$, this tells us that k is odd and there are an odd number of primes above 19. Hence,

$$w(E/\mathbb{Q}(\sqrt[3^n]{m})) = (-1)^{\text{odd number}} \cdot (-1)^{n+1} = (-1)^n,$$

since $\mathbb{Q}(\sqrt[3^n]{m})$ has an even number of infinite places when n is odd and an odd number when n is even. Since the sign of the global root number changes at each step, the parity conjecture implies that the rank of E must grow at every step of the tower $(\mathbb{Q}(\sqrt[3^n]{m}))_{n\geqslant 0}$. In particular, the rank of E over $\mathbb{Q}(\sqrt[3^n]{m})$ is at least n.

In [27], Example 3.12 is generalised to the setting of root numbers of elliptic curves defined over $\mathbb{Q}$ in the towers of extensions $(\mathbb{Q}(\sqrt[p^n]{m}))_{n\geqslant 0}$ and $(\mathbb{Q}(\zeta_{p^n}, \sqrt[p^n]{m}))_{n\geqslant 0}$, where p is an odd prime. Here, we present the results in the setting of semistable elliptic curves.

Theorem 3.13 ([27], Theorem 6). *Let E be a semistable elliptic curve over $\mathbb{Q}$. Let p be an odd prime at which E has good reduction. Let $m > 1$ be an p-th power free integer.*[†] *Then the global root number for E over $K = \mathbb{Q}(\sqrt[p^n]{m})$ is*

$$w(E/K) = w(E/\mathbb{Q}) \cdot (-1)^{n(\frac{p-1}{2}+t)},$$

where t is the number of primes of multiplicative reduction of E that do not divide m and that are non-squares modulo p.

Corollary 3.14. *Let E be a semistable elliptic curve over $\mathbb{Q}$ and let $p \equiv 3 \pmod 4$ be a prime at which E has good reduction. Suppose that every prime of multiplicative reduction is a square modulo p. If the parity conjecture holds then the rank of E over $\mathbb{Q}(\sqrt[p^n]{m})$ is at least n for every p-th power-free integer m.*

Proof. Since $w(E/\mathbb{Q}(\sqrt[p^n]{m})) = w(E/\mathbb{Q}) \cdot (-1)^n$, assuming the parity conjecture the rank of E increases at every step of the tower of number fields $(\mathbb{Q}(\sqrt[p^n]{m}))_{n\geqslant 0}$. □

Example 3.15. Assuming the parity conjecture, the curve

$$E : y^2 + y = x^3 - x^2 \quad \text{(11A3)}$$

has rank at least n over $\mathbb{Q}(\sqrt[7^n]{m})$ for any positive 7-th power-free integer m. Indeed, we have $\Delta_E = -11$ and E has split multiplicative reduction at 11. Since 11 is a square modulo 7, the rank is at least n over $\mathbb{Q}(\sqrt[7^n]{m})$. In particular, the parity conjecture implies that E has rank at least 1 over $\mathbb{Q}(\sqrt[7]{3})$. Magma fails to find the point of infinite order on $E/\mathbb{Q}(\sqrt[7]{3})$.

[†] We call m 'p-th power free' if $x^p \nmid m$ for any x, i.e. it is the generalisation of square-free and cube-free.

3.6 | $E : y^2 + y = x^3 + x^2 + x$ has rank at least 3^n over $\mathbb{Q}(\zeta_{3^n}, \sqrt[3^n]{m})$

Example 3.16. Let us study what happens to the rank of the curve $E : y^2 + y = x^3 + x^2 + x$ (19A3) from Examples 3.10 and 3.12 over $K_n = \mathbb{Q}(\zeta_{3^n}, \sqrt[3^n]{m})$. We claim that, assuming the parity conjecture for twists (see §2.4), E has rank at least 3^n over $\mathbb{Q}(\zeta_{3^n}, \sqrt[3^n]{m})$, for every cube-free integer $m > 1$. Let $G = \mathrm{Gal}(K_n/\mathbb{Q})$ and $V = E(K_n) \otimes_{\mathbb{Z}} \mathbb{C}$. Then, by Lemma 2.17, for any subgroup $H \leqslant \mathrm{Gal}(K_n/\mathbb{Q})$, we have

$$\mathrm{rk}(E/K_n^H) = \langle \mathrm{Ind}_H^G \mathbb{1}, V \rangle_G.$$

We can use this, along with our knowledge from Example 3.12 about what happens to E over $\mathbb{Q}(\sqrt[3^n]{m})$, to say something about the rank of E over K_n. Firstly, note that

$$\sigma_n = \mathrm{Ind}^G_{\mathrm{Gal}(K_n/\mathbb{Q}(\sqrt[3^n]{m}))} \mathbb{1} = \mathbb{1} \oplus \rho_1 \cdots \oplus \rho_n,$$

where ρ_k is an irreducible representation of dimension $p^{k-1}(p-1)$, see [27] §5.2 for more details. By Theorem 2.16, we have

$$w(E/\mathbb{Q}(\sqrt[3^n]{m})) = w(E/\mathbb{Q}) \cdot w(E/\mathbb{Q}, \rho_1) \cdots w(E/\mathbb{Q}, \rho_n),$$

whence, $w(E/\mathbb{Q}, \rho_k) = -1$ as we saw in Example 3.12 that $w(E/\mathbb{Q}) = +1$ and $w(E/\mathbb{Q}(\sqrt[3^n]{m})) = (-1)^n$. Assuming the parity conjecture for twists, this tells us that ρ_k appears in V with odd multiplicity for all $k \in \{1, \dots, n\}$. Now, $\mathbb{C}[G]$ has $\dim \rho_k$ copies of ρ_k, whereby $\mathrm{rk}(E/K_n) = \langle \mathbb{C}[G], V \rangle_G$ is at least $\sum_{k=1}^n \dim \rho_k = 3^n - 1$. Note that $w(E/\mathbb{Q}(\zeta_3)) = -1$ since 19 splits in $\mathbb{Q}(\zeta_3)$, so the parity conjecture implies $\mathrm{rk}(E/\mathbb{Q}(\zeta_3)) \geqslant 1$ and, in particular,

$$\mathrm{rk}(E/\mathbb{Q}(\zeta_3)) = \langle \mathbb{C}[\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})], V \rangle_G \geqslant 1.$$

Since $\mathbb{C}[\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})]$ appears in $\mathbb{C}[G]$ and is orthogonal to the ρ_k, along with our previous working this tells us that

$$\mathrm{rk}(E/K_n) = \langle \mathbb{C}[G], V \rangle_G \geqslant 3^n.$$

Remark 3.17. By Lemma 2.18, the result in the above example could have been deduced from the parity conjecture for E over intermediate fields rather than the parity conjecture for twists.

In [27], the methods demonstrated in the example above are generalised in order to prove the following result (which for simplicity we state just for semistable elliptic curves).

Theorem 3.18 ([27], Corollary 13). *Let $p \equiv 3 \pmod 4$ be a prime number and let E be a semistable elliptic curve with good reduction at p and such that every prime of multiplicative reduction is a square modulo p. If the parity conjecture holds then, for every p-th powerfree integer $m > 1$, the rank of E over $\mathbb{Q}(\zeta_{p^n}, \sqrt[p^n]{m})$ is at least p^n.*

Example 3.19. Assuming the parity conjecture, the curve $E : y^2 + y = x^3 - x^2$ (11A3) from Example 3.15 has rank at least 7^n over $\mathbb{Q}(\zeta_{7^n}, \sqrt[7^n]{m})$, for any 7-th power free integer $m > 1$.

Remark 3.20. For a possible approach to explaining these points of infinite order using Heegner points, see [12].

3.7 | Every positive $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ can be represented by $x^3 - 91x - 182$

Theorem 2.13 tells us that half of the quadratic twists of an elliptic curve over $\mathbb{Q}$ by d have global root number $+1$ and half have global root number -1. This distribution can be such that the root number is determined only by the sign of d, and a description of elliptic curves $E/\mathbb{Q}$ for which this occurs can be found in [16, Theorem 1.1]. If we believe the parity conjecture, we can use this to deduce that every positive rational number d can be written in the form $d = s^2(t^3 - 91t - 182)$ for s and t in $\mathbb{Q}$. For example, letting $f(x) = x^3 - 91x - 182$:

$$1 = \frac{1}{8^2} \cdot f(-3), \qquad 2 = \frac{27^2}{16^2} \cdot f\left(-\frac{19}{9}\right), \qquad 3 = \frac{9^2}{64^2} \cdot f\left(-\frac{17}{3}\right), \qquad 5 = \frac{675^2}{1\,185\,848^2} \cdot f\left(\frac{11\,209}{45}\right).$$

It is not clear how one might prove this property of $f(x)$ without the parity conjecture.

Example 3.21 (As in [16], Example 4). We claim that all positive quadratic twists of the curve

$$E : y^2 = x^3 - 91x + 182 \quad (8281\text{H}1)$$

have root number $+1$ and all negative quadratic twists have root number -1. The minimal discriminant of E is $\Delta = 7^2 \cdot 13^2$ and E has type II reduction at both primes. By Theorem 2.3, $w(E/\mathbb{Q}_7) = (-1)^{\lfloor \frac{2\cdot 7}{12} \rfloor} = -1$ and similarly $w(E/\mathbb{Q}_{13}) = +1$. Hence, $w(E/\mathbb{Q}) = +1$. Let $d \in \mathbb{Q}^\times \backslash \mathbb{Q}^{\times 2}$, $K = \mathbb{Q}(\sqrt{d})$ and let v denote a prime above 7 in K. If 7 is ramified in K, then

$$w(E/K_v) = (-1)^{\lfloor \frac{4\cdot 7}{12} \rfloor} = +1.$$

By a similar calculation, if 7 is inert in K, then $w(E/K_v) = +1$. If 7 splits, by Lemma 2.8, there are two distinct places with the same root number. In all cases, $\prod_{v|7} w(E/K_v) = +1$. We can do the same calculation for $\tilde{v}$ above 13 to find $\prod_{\tilde{v}|13} w(E/K_{\tilde{v}}) = +1$. Thus,

$$w(E/K) = \begin{cases} +1 & \text{if } d > 0; \\ -1 & \text{if } d < 0, \end{cases}$$

and our claim follows from Lemma 2.10. In particular, the parity conjecture implies that all negative quadratic twists of E have infinitely many points.

Definition 3.22. We say that $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ can be represented by $f(x) \in \mathbb{Q}[x]$ if there exists an $s \in \mathbb{Q}^\times$ and $t \in \mathbb{Q}$ such that $d = s^2 f(x)$. If $f(x)$ is a cubic and the quadratic twist of the elliptic curve $E : y^2 = f(x)$ by $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ has positive rank, then d is represented by $f(x)$.

Example 3.23. Let

$$E : y^2 = x^3 - 91x - 182. \quad (132496\text{E}1)$$

This is the quadratic twist by −1 of the curve in Example 3.21 so

$$w(E_d/\mathbb{Q}) = \begin{cases} -1 & \text{for } d > 0; \\ +1 & \text{for } d < 0. \end{cases}$$

The parity conjecture implies that every positive $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is representable by $x^3 - 91x - 182$.

Remark 3.24. Assuming Goldfeld's conjecture that there is a 50/50 distribution of the rank of quadratic twists of an elliptic curve $E/\mathbb{Q}$ being 0 and 1, from Example 3.23, we deduce[†] that 0% of negative integers (up to squares) can be represented by $x^3 - 91x - 182$. This is a peculiar property for a cubic polynomial: its positive values hit all possible classes modulo squares, whereas its negative values hit a very sparse set.

3.8 | Every $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ can be represented by $4x^3 - 32x - 35$ or $9x^3 + 16x + 16$

Examples 3.23 and 3.21 show that, assuming the parity conjecture, for every $d \in \mathbb{Q}$ at least one of the equations

$$d \cdot y^2 = x^3 - 91x + 182 \qquad \text{and} \qquad d \cdot y^2 = x^3 - 91x - 182$$

has a rational solution. In particular, every $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ can be represented by $x^3 - 91x + 182$ or $x^3 - 91x - 182$. It turns out that every cubic $f(x)$ has an auxiliary cubic $g(x)$ with this property.

Theorem 3.25. *Let $f(x) \in \mathbb{Q}[x]$ be a separable cubic polynomial. Assuming the parity conjecture, there exists a separable cubic polynomial $g(x) \in \mathbb{Q}[x]$ such that every $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is represented by $f(x)$ or $g(x)$.*

Proof. Take $g(x) = d_0 f(x)$, where $d_0 < 0$ is such that all primes of bad reduction of $E : y^2 = f(x)$ split in $\mathbb{Q}(\sqrt{d_0})$. Then $E_{d_0} : y^2 = g(x) = d_0 f(x)$ is the quadratic twist of E by d_0. By the proof of Theorem 2.13(ii), for any $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, the root number of the quadratic twists of E_{d_0} and E by d satisfy $w(E_{dd_0}/\mathbb{Q}) = -w(E_d/\mathbb{Q})$. The parity conjecture implies that at least one of E_d and E_{dd_0} has a point of infinite order, and thus, every $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is represented by $f(x)$ or $g(x)$. □

We can also find examples of such curves that are not quadratic twists of each other.

Example 3.26. Let

$$E : y^2 = x^3 + 16x^2 - 3072x - 68\,608.$$

By similar calculations to those in Example 3.21, all the positive quadratic twists of the curve have root number +1 over $\mathbb{Q}$, and all the negative quadratic twists have root number −1. Thus, every $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ can be represented by $x^3 - 91x - 182$ or by $x^3 + 16x^2 - 3072x - 68\,608$.

[†] None of the quadratic twists of E have torsion points as Galois has maximal image on $E[p]$ for all $p > 2$ and $E(\mathbb{Q})[2] = 0$.

Theorem 2.13 tells us that the global root number in a quadratic twist family is periodic; we can use this to come up with curves that are not quadratic twists of each other, for which one of their quadratic twists always has root number −1 and where the root number does not only depend on the sign of d.

Example 3.27. Let E and E' be given by

$$E : y^2 = 4x^3 - 32x - 35 \quad \text{and} \quad E' : y^2 = 9x^3 + 16x + 16.$$

We claim that for every $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, either $w(E_d/\mathbb{Q}) = -1$ or $w(E'_d/\mathbb{Q}) = -1$.

Both E and the quadratic twist E'_{-3} have minimal discriminant −307 and split multiplicative reduction at 307. Thus, $w(E/\mathbb{Q}) = w(E'_{-3}/\mathbb{Q}) = +1$. Since $307 \equiv 1 \pmod 3$, $\mathbb{Q}_{307}$ contains $\sqrt{-3}$ and so 307 has the same splitting behaviour in $\mathbb{Q}(\sqrt{d})$ as it does in $\mathbb{Q}(\sqrt{-3d})$. Thus, $w(E/\mathbb{Q}(\sqrt{d})) = -w(E'_{-3}/\mathbb{Q}(\sqrt{-3d}))$ by Corollary 2.5 and, by Lemma 2.10, $w(E_d/\mathbb{Q}) = -w(E'_d/\mathbb{Q})$. This proves the claim. The parity conjecture implies that every $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ can be represented as $f(x) = 4x^3 - 32x - 35$ or $g(x) = 9x^3 + 16x + 16$.

Remark 3.28. This representation of $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ as one of two cubics can be given by values of x with very large height. In Example 3.27, the 'smallest' (in terms of the height of x) representation of −17 is

$$-17 = \frac{223\,280\,590\,408\,502\,625\,944\,275\,649\,356\,615\,800\,897^2}{6\,034\,892\,905\,593\,758\,120\,664\,851\,652\,128\,224\,164\,489^2} \cdot g\left(-\frac{330\,029\,825\,965\,445\,476\,649\,347\,569}{29\,773\,633\,899\,834\,719\,965\,546\,857}\right).$$

3.9 | All quadratic twists of $y^2 = x^3 + \frac{5}{4}x^2 - 2x - 7$ over $\mathbb{Q}(\zeta_3, \sqrt[3]{11})$ have infinitely many points

As mentioned at the end of §2.3, the 50/50 distribution of root numbers of quadratic twists of elliptic curves over $\mathbb{Q}$ can fail quite dramatically over number fields; there are elliptic curves over number fields for which all quadratic twists have the same root number.

Example 3.29 (As considered in [21]). Let $K = \mathbb{Q}(\zeta_3, \sqrt[3]{11})$. We claim that all quadratic twists of the curve

$$E : y^2 = x^3 + \frac{5}{4}x^2 - 2x - 7$$

over K have root number −1 and so should have positive rank. Indeed, the minimal discriminant of $E/\mathbb{Q}$ is 11^4, and E acquires everywhere good reduction over K. Since K has three complex places and $K(\sqrt{d})$ has six, for $d \in K^\times \setminus K^{\times 2}$, we have $w(E/K) = -1$ and $w(E/K(\sqrt{d})) = +1$. By Lemma 2.10,

$$w(E_d/K) = w(E/K(\sqrt{d}))w(E/K) = -1.$$

So, assuming the parity conjecture, E_d has a point of infinite order for every $d \in K^\times$. See Theorem 3.33 below for a more general result concerning this behaviour.

Remark 3.30. Example 3.29 shows that, assuming the parity conjecture, the polynomial $x^3 + 5/4x^2 - 2x - 7$ takes every value in $K^\times/K^{\times 2}$.

3.10 | $E : y^2 = x^3 + x^2 - 12x - \frac{67}{4}$ has even rank over every field extension of $\mathbb{Q}(\sqrt[4]{-37})$

Consider the elliptic curve

$$E : y^2 = x^3 + x.$$

It has complex multiplication defined over $K = \mathbb{Q}(i)$ with $\mathrm{End}_K(E) \cong \mathbb{Z}[i]$, where i acts by $[i] \cdot (x, y) = (-x, iy)$. The rank of E over K is even, and similarly, $\mathrm{rk}(E/F)$ is even for any extension F of K, since $E(F) \otimes_{\mathbb{Z}} \mathbb{Q}$ is naturally a $\mathbb{Q}(i)$-vector space, and so has even dimension over $\mathbb{Q}$. Moreover, using the fact that $\mathrm{rk}(E_d/K) = \mathrm{rk}(E/K(\sqrt{d})) - \mathrm{rk}(E/K)$, we see that $\mathrm{rk}(E_d/K)$ is even for any $d \in K^\times$. The parity conjecture forces some non-CM elliptic curves to exhibit the same behaviour.

Example 3.31 (As considered in [21]). Let us take the curve

$$E : y^2 = x^3 + x^2 - 12x - \frac{67}{4}. \quad (1369\mathrm{E}1)$$

Then $\Delta_E = 37^3$ and $j(E) = 2^{12}$, so $E/\mathbb{Q}$ has potentially good reduction at 37 and it has everywhere good reduction over $K = \mathbb{Q}(\sqrt[4]{-37})$ and over every extension F of K. Since F has an even number of infinite places, $w(E/F) = +1$. In particular, assuming the parity conjecture, E has even rank over every extension of K.

Remark 3.32. Such a field K exists for every elliptic curve E with integral j-invariant as this means that E has potentially good reduction everywhere, so we can find an extension of the base field over which E acquires everywhere good reduction.

As in §3.1 and §3.2, one would hope that there is some extra structure analogous to complex multiplication that would explain why E always has even rank over extensions of K in Example 3.31. However, it is not clear how to prove this behaviour of ranks for any non-CM curve without assuming the parity conjecture. Elliptic curves that display this phenomenon, and that described in §3.9, are classified by the following theorem.

Theorem 3.33 ([21], Theorem 1). *For an elliptic curve E over a number field K, the following are equivalent.*

(i) *All quadratic twists of E/K have the same root number.*
(ii) *$w(E/F) = w(E/K)^{[F:K]}$ for every finite extension F of K.*
(iii) *K has no real places, and E acquires everywhere good reduction over an abelian extension of K.*

Theorem 3.33 tells us that if E/K satisfies (*iii*) and $w(E/K) = +1$, then, assuming the parity conjecture, E will have even rank over every extension of K.

Remark 3.34. It turns out that the criteria in Theorem 3.33 are equivalent to K having no real places, and for all primes ℓ and all places $v \nmid \ell$ of K, the action of the absolute Galois group of K_v on the Tate module $T_\ell(E)$ being abelian (see [21]). This is another way in which E resembles a CM curve, since (in view of the Tate conjecture) an elliptic curve has CM if and only if the action of the global absolute Galois group on the ℓ-adic Tate module is abelian.

3.11 | The rank of $E : y^2 + xy = x^3 - x^2 - 2x - 1$ grows in extensions of $\mathbb{Q}(\sqrt{-1})$ of even degree

Theorem 3.33 tells us that there exist elliptic curves over number fields for which all quadratic twists have the same root number. We can also use the theorem to come up with examples of elliptic curves E/K whose rank grows in every even degree extension of K.

Example 3.35 (As considered in [21]). Let

$$E : y^2 + xy = x^3 - x^2 - 2x - 1. \quad (49A1)$$

We have $\Delta_E = -7^3$, $j(E) = -3^3 \cdot 5^3$ and E has additive, potentially good, type III reduction at 7. We claim that the rank of E must grow in every extension of $K = \mathbb{Q}(\sqrt{-1})$ of even degree. Indeed, 7 is inert in $\mathbb{Q}(\sqrt{-1})$ and by Theorem 2.3, $w(E/K_v) = +1$, where v is the unique prime above 7 in K, and so, $w(E/K) = -1$. Note that K has no real places and E acquires everywhere good reduction over $\mathbb{Q}(\sqrt{-1}, \sqrt[4]{7})$, which is an abelian extension of K. By Theorem 3.33, for any even degree extension F of K,

$$w(E/F) = w(E/K)^{[F:K]} = (-1)^{\text{even number}} = +1 \neq w(E/K),$$

and the parity conjecture predicts that $\mathrm{rk}(E/F) > \mathrm{rk}(E/K)$.

3.12 | Every positive integer $n \equiv 5, 6$ or $7 \pmod 8$ is a congruent number

The classical *congruent number problem* asks: for a natural number n, can it be realised as the area of a right-angled triangle with rational sides? We call such n *congruent numbers*. The congruent number problem dates back to Arab manuscripts from the 10th century and, to this day, it is not known in full generality, although it has been extensively studied. Heegner [37] proved that if p is a prime congruent to 5 modulo 8, then it is a congruent number, and other cases have been proved using the theory of Heegner points on modular curves, see [70]. Smith [65] has announced a proof that at least 55.9% of positive square-free integers congruent to 5, 6 or 7 modulo 8 are congruent numbers. Kriz has announced a proof that 100% of such integers are congruent numbers and 100% of those congruent to 1, 2 or 3 are not congruent numbers (see [45, Theorem 10.17]). It has been long expected that every positive integer congruent to $5, 6$ or $7 \pmod 8$ is a congruent number, and we will explain how this can be deduced from the parity conjecture.

Example 3.36. There is a right-angled triangle with sides of length 3, 4, 5 which has area 6, so that 6 is a congruent number. Similarly, the right-angled triangle with sides of length $\frac{35}{12}$, $\frac{24}{5}$ and $\frac{337}{60}$ has area 7, whence 7 is a congruent number.

Definition 3.37. The elliptic curve $E : y^2 = x^3 - x$ is called the *congruent number curve* because the quadratic twist of the curve by $n \in \mathbb{N}$, $E_n : y^2 = x(x-n)(x+n)$, has a point of infinite order over $\mathbb{Q}$ if and only if n is a congruent number (see, e.g. [71] for details on why this is the case). For these elliptic curves, a rational point (x, y) has infinite order if and only if $y \neq 0$.

Example 3.38. We already know that 7 is a congruent number. Indeed, the elliptic curve

$$E_7 : y^2 = x(x-7)(x+7)$$

has a rational point of infinite order, namely (25,120).

Example 3.39. There is a point on the curve

$$E_{166} : y^2 = x(x-166)(x+166),$$

which is given by

$$x = -\frac{7\,969\,693\,283}{98\,823\,481} \text{ and } y = -\frac{1\,280\,060\,076\,599\,271}{982\,404\,224\,621}.$$

This tells us that 166 is a congruent number. The height of the generator E_{166} is already very large. What if we wanted to know whether 800 006 was a congruent number? Magma [3] cannot find a point of infinite order on $E_{800\,006}$ and cannot tell us whether 800 006 is not a congruent number. Assuming the parity conjecture, we can easily show that it is.

Theorem 3.40. *Let n be a positive, square-free integer. Then*

$$w(E_n/\mathbb{Q}) = \begin{cases} +1 & \textit{if}\, n \equiv 1,\ 2\ \textit{or}\ 3 \pmod 8, \\ -1 & \textit{if}\, n \equiv 5,\ 6\ \textit{or}\ 7 \pmod 8. \end{cases}$$

Proof. By Theorem 2.13(i), $w(E_n/\mathbb{Q})$ depends only on $n \pmod{16}$. So, all one needs to do is calculate the root numbers for one square-free n in each of the congruence classes modulo 16. For $E_1 : y^2 = x^3 - x$, we have $c_4 = 2^4 \cdot 3$, $c_6 = 0$ and $\Delta_{E_1} = 2^6$. In the terminology of Notation A.1, we have $c_4' = 3$ and $c_4' - 4c_{6,7} = 3$ so that, by the table in the Appendix, $w(E_1/\mathbb{Q}_2) = -1$ and hence $w(E_1/\mathbb{Q}) = +1$. For $E_5 : y^2 = x^3 - 25x$, we have $c_4 = 2^4 \cdot 3 \cdot 5^2$, $c_6 = 0$, $\Delta_{E_5} = 2^6 \cdot 5^6$, $c_4' = 75 \equiv 3 \pmod 4$ and $c_4' - 4c_{6,7} \equiv 11 \pmod{16}$. Again, by the table, $w(E_5/\mathbb{Q}_2) = +1$. By Theorem 2.3, $w(E_5/\mathbb{Q}_5) = (-1)^{\lfloor \frac{6\cdot 5}{12} \rfloor} = +1$, so $w(E_5/\mathbb{Q}) = -1$. Similarly, we have

$$w(E_{41}/\mathbb{Q}) = w(E_2/\mathbb{Q}) = w(E_{10}/\mathbb{Q}) = w(E_3/\mathbb{Q}) = w(E_{11}/\mathbb{Q}) = +1;$$

$$w(E_{13}/\mathbb{Q}) = w(E_6/\mathbb{Q}) = w(E_{14}/\mathbb{Q}) = w(E_7/\mathbb{Q}) = w(E_{15}/\mathbb{Q}) = -1,$$

which completes the proof. □

Corollary 3.41. *Assuming the parity conjecture, every square-free positive integer* $n \equiv 5, 6,$ *or* $7 \pmod 8$ *is the area of a right-angled triangle with rational sides.*

We can deduce immediately from this corollary that, assuming the parity conjecture, 800 006 is a congruent number. Stephens was the first to apply parity-type conjectures to the congruent number problem [67] and proved that Selmer's second conjecture (see §1.2) implies that positive integers $n \equiv 5, 6, 7 \pmod 8$ are congruent numbers.

3.13 | $\mathscr{E} : y^2 = x(x^2 - 49(1 + t^4)^2)$ has a point of infinite order for every $t \in \mathbb{Q}$ but rk $\mathscr{E}/\mathbb{Q}(t) = 0$

One incentive for studying root numbers is to study ranks in families of elliptic curves. Consider a one parameter family of elliptic curves

$$\mathscr{E} : y^2 = x^3 + A(t)x + B(t),$$

for some fixed $A(t), B(t) \in \mathbb{Q}(t)$, where $\Delta_{\mathscr{E}} \neq 0$. A point of infinite order over $\mathbb{Q}(t)$ gives a parametric family of points over the fibres $\mathscr{E}_t$. A natural question to ask is 'if every fibre has positive rank, does it mean there is a point of infinite order over $\mathbb{Q}(t)$?' Assuming the parity conjecture, the answer is 'no'.

Theorem 3.42 (As considered in [6]). *Let* $\mathscr{E} : y^2 = x(x^2 - 49(1 + t^4)^2)$. *Then*

(i) rk $\mathscr{E}/\mathbb{Q}(t) = 0$;
(ii) *assuming the parity conjecture, for every* $t \in \mathbb{Q}$, *the fibre* $\mathscr{E}_t$ *has* $\operatorname{rk}(\mathscr{E}_t/\mathbb{Q}) \geqslant 1$.

Proof. In [6], it is shown that $\mathscr{E} : y^2 = x(x^2 - 49(1 + t^4)^2)$ has rank 0 over $\mathbb{Q}(t)$. For (*ii*), let $t = l/m$ where $(l, m) = 1$. Then $\mathscr{E}_t$ is isomorphic to a curve of the form

$$y^2 = x(x - n)(x + n)$$

over $\mathbb{Q}$, where $n = 7l^4 + 7m^4$. Clearly, $n \equiv 6$ or $7 \pmod 8$ so, by Theorem 3.40, $w(\mathscr{E}_t/\mathbb{Q}) = -1$. □

The family $\mathscr{E}$ in Theorem 3.42 has constant j-invariant. In [15, Theorem 1.2], Desjardins proved that, for a family with non-constant j-invariant, assuming Chowla's conjecture and the Squarefree conjecture (see [15, Conjectures 2.1 and 2.7]), the function $t \mapsto w(\mathscr{E}_t/\mathbb{Q})$ is never constant. She used this to prove that the sets

$$W_+ = \{t \in \mathbb{P}^1 : w(\mathscr{E}_t/\mathbb{Q}) = +1\},$$
$$W_- = \{t \in \mathbb{P}^1 : w(\mathscr{E}_t/\mathbb{Q}) = -1\}$$

are infinite, and so, assuming the parity conjecture, the rational points $\mathscr{E}(\mathbb{Q})$ are Zariski dense in $\mathscr{E}$.

Since the sets W_+ and W_- are infinite when the j-invariant is non-constant, one might expect that the root numbers are equidistributed and that the average root number is 0. This is not always the case, as shown in [38], where Helfgott proved that if $\mathcal{E}$ has no places of multiplicative reduction, the average root number need not be zero.

For a family with non-constant j-invariant, if one restricts to $t \in \mathbb{Z}$, the function $t \mapsto w(\mathcal{E}_t/\mathbb{Q})$ may be constant. For example, in [54], it is shown that the surface

$$\mathcal{E} : y^2 = x^3 + tx^2 - (t+3)x + 1$$

has $w(\mathcal{E}_t/\mathbb{Q}) = -1$ for every $t \in \mathbb{Z}$. This example was first investigated by Washington [72] who proved via 2-descent that, for every $t \in \mathbb{Z}$ such that $t^2 + 3t + 9$ is square free and assuming the finiteness of the Tate–Shafarevich group, the rank of $\mathcal{E}_t$ is odd.

3.14 | $y^2 + y = x^3 - x$ acquires new solutions over $K(\sqrt{\Delta_K})$ whenever $37 \nmid \Delta_K$ and $\sqrt{\Delta_K} \notin K$

We saw in §3.5 and §3.6 that the parity conjecture can predict the growth of the rank of elliptic curves in towers of fields of the form $\mathbb{Q}(\sqrt[p^n]{m})$ and $\mathbb{Q}(\zeta_{p^n}, \sqrt[p^n]{m})$. The parity conjecture also predicts that the rank of an elliptic curve over $\mathbb{Q}$ can grow in many generic number fields.

Theorem 3.43. *Let K be any number field that does not contain $\sqrt{\Delta_K}$ and set $F = K(\sqrt{\Delta_K})$. Assuming the parity conjecture, every $E/\mathbb{Q}$ with $w(E/\mathbb{Q}) = -1$ and $(N_E, \Delta_K) = 1$ has* $\mathrm{rk}(E/F) > \mathrm{rk}(E/\mathbb{Q})$.

Proof. Let $\tilde{K}/\mathbb{Q}$ be the Galois closure of $K/\mathbb{Q}$, $G = \mathrm{Gal}(\tilde{K}/\mathbb{Q})$ and $H = \mathrm{Gal}(\tilde{K}/K)$. Write $\mathrm{Ind}_H^G \mathbb{1} = \mathbb{1} \oplus \rho$ and ϵ for the nontrivial character of $\mathrm{Gal}(\mathbb{Q}(\sqrt{\Delta_K})/\mathbb{Q})$. By Frobenius reciprocity (see Lemma 2.17),

$$\mathrm{rk}(E/F) = \langle \mathrm{Ind}^G_{\mathrm{Gal}(\tilde{K}/F)} \mathbb{1}, E(\tilde{K}) \otimes_{\mathbb{Z}} \mathbb{C} \rangle.$$

Note that

$$\mathrm{Ind}^G_{\mathrm{Gal}(\tilde{K}/F)} \mathbb{1} = \mathrm{Ind}^G_H(\mathbb{1} \oplus \mathrm{Res}^G_H \epsilon) = \mathbb{1} \oplus \rho \oplus \epsilon \oplus (\epsilon \otimes \rho)$$

so, assuming the parity conjecture for twists, it will suffice to show that one of $w(E/\mathbb{Q}, \rho)$, $w(E/\mathbb{Q}, \epsilon)$ and $w(E/\mathbb{Q}, \epsilon \otimes \rho)$ is -1. In fact, by Lemma 2.18, it suffices to assume the parity conjecture for E over the subfields of $\tilde{K}$.

Let $K = \mathbb{Q}(\alpha)$. The permutation action of G on the cosets of H agrees with the permutation action on the Galois conjugates of α, since both actions are transitive with H as a point-stabiliser. Even permutations are precisely those fixing $\sqrt{\Delta_K}$, and therefore, $\det(\mathrm{Ind}_H^G \mathbb{1}) = \det \rho$ cuts out the extension $\mathbb{Q}(\sqrt{\Delta_K})/\mathbb{Q}$ so that $\det \rho = \epsilon$. It follows that $\det(\epsilon \otimes \rho) = \epsilon^{\otimes \dim \rho} \otimes \det \rho$ is either $\mathbb{1}$ or ϵ if $\dim \rho$ is odd or even, respectively. By Theorem 2.15, if $[K : \mathbb{Q}]$ is even, then $\dim \rho$ is odd and $w(E/\mathbb{Q}, \epsilon \otimes \rho) = w(E/\mathbb{Q})^{\dim \rho} = -1$. Similarly, if $[K : \mathbb{Q}]$ is odd, then $\dim \rho$ is even and $w(E/\mathbb{Q}, \rho) w(E/\mathbb{Q}, \epsilon) = w(E/\mathbb{Q}, \rho \oplus \epsilon) = w(E/\mathbb{Q})^{\dim \rho + 1} = -1$. □

Remark 3.44. Theorem 3.43 applies to generic extensions $K/\mathbb{Q}$. If $[K : \mathbb{Q}] = n > 2$ and the Galois closure of K over $\mathbb{Q}$ has Galois group S_n, then K does not contain $\sqrt{\Delta_K}$. We therefore expect the rank of every $E/\mathbb{Q}$ with $w(E/\mathbb{Q}) = -1$ to increase in splitting fields of most polynomials.

3.15 | $E : y^2 + y = x^3 - x$ has rank at least 434 over any S_{14}-extension $K/\mathbb{Q}$ with $37 \nmid \Delta_K$

Example 3.45. Let $E/\mathbb{Q}$ be an elliptic curve with $w(E/\mathbb{Q}) = -1$ and let F be an S_5-extension of $\mathbb{Q}$ with $(N_E, \Delta_F) = 1$. We claim that $\mathrm{rk}(E/F) \geqslant 6$. Indeed, S_5 has seven irreducible representations, all of which are self-dual. These are the trivial representation $\mathbb{1}$, sign representation ϵ, two 4-dimensional representations ρ_1 and $\rho_2 = \rho_1 \otimes \epsilon$, two 5-dimensional representations τ_1 and $\tau_2 = \tau_1 \otimes \epsilon$ and one 6-dimensional representation σ. We can write

$$E(F) \otimes_{\mathbb{Z}} \mathbb{C} = \mathbb{1}^{\oplus a} \oplus \epsilon^{\oplus b} \oplus \rho_1^{\oplus c} \oplus \rho_2^{\oplus d} \oplus \tau_1^{\oplus e} \oplus \tau_2^{\oplus f} \oplus \sigma^{\oplus g}.$$

Since $\mathrm{rk}(E/F) = \dim(E(F) \otimes_{\mathbb{Z}} \mathbb{C})$,

$$\mathrm{rk}(E/F) = a + b + 4c + 4d + 5e + 5f + 6g.$$

Now, $\det(\tau_1 \otimes \epsilon) = \epsilon^{\otimes \dim \tau_1} \otimes \det \tau_1$, so either $\det(\tau_1) = \mathbb{1}$ or $\det(\tau_2) = \mathbb{1}$. By Theorem 2.15,

$$w(E/\mathbb{Q}, \tau_1) = -1 \quad \text{or} \quad w(E/\mathbb{Q}, \tau_2) = -1.$$

By assumption, we have $w(E/\mathbb{Q}, \mathbb{1}) = w(E/\mathbb{Q}) = -1$ so, assuming the parity conjecture for twists, a is odd and either e or f is odd. Hence, $\mathrm{rk}(E/F) \geqslant 6$.

Theorem 3.46. *Let $E/\mathbb{Q}$ be an elliptic curve with $w(E/\mathbb{Q}) = -1$. Assume the parity conjecture for twists.*

(i) *Let ρ be an odd-dimensional irreducible self-dual Artin representation with* $\det \rho = \mathbb{1}$ *and whose conductor is coprime to N_E. Then $\langle \rho, E(F) \otimes_{\mathbb{Z}} \mathbb{C} \rangle > 0$, where ρ factors through $F/\mathbb{Q}$.*

(ii) *For a Galois extension $F/\mathbb{Q}$ with $(N_E, \Delta_F) = 1$,*

$$\mathrm{rk}(E/F) \geqslant \frac{k}{m},$$

where k is the sum of dimensions of the odd-dimensional irreducible self-dual representations of $\mathrm{Gal}(F/\mathbb{Q})$ *and m is the number of one-dimensional representations of* $\mathrm{Gal}(F/\mathbb{Q})$ *of order 1 or 2.*

Proof. (i) This follows immediately from Theorem 2.15. (ii) Let $G = \mathrm{Gal}(K/\mathbb{Q})$ and let ρ be any irreducible odd-dimensional self-dual representation of G. Denote the order two 1-dimensional representations of G by $\epsilon_1, \dots, \epsilon_{m-1}$. Since ρ is odd-dimensional, taking $\epsilon = \det \rho$, we obtain $\det(\rho \otimes \epsilon) = \epsilon^{\otimes \dim \rho} \otimes \det \rho = \mathbb{1}$. We also have $\det(\rho \otimes \epsilon \otimes \epsilon_i) = \epsilon_i$ for $i = 1, \dots, m-1$. Thus, the odd-dimensional irreducible self-dual representations come in sets of size m, each with the same dimension and different determinant character $\mathbb{1}, \epsilon_1, \dots, \epsilon_{m-1}$. By (i), $\rho \otimes \epsilon$ appears in $E(F) \otimes_{\mathbb{Z}} \mathbb{C}$ and the result follows. □

Remark 3.47. Theorem 3.46 implies that for a fixed elliptic curve $E/\mathbb{Q}$ with $w(E/\mathbb{Q}) = -1$, every odd-dimensional irreducible self-dual Artin representation which has trivial determinant and whose conductor is coprime to N_E must appear in the Mordell–Weil group of E over an extension of $\mathbb{Q}$.

To generalise Example 3.45 to finding a lower bound on the rank of E over an S_n-extension of $\mathbb{Q}$, we need to understand the odd-dimensional irreducible representations of S_n. For a given n, the dimensions of the irreducible representations of S_n can be calculated using the Young tableaux, see [30, p. 50]. We will instead use a known case of the McKay conjecture to find a crude lower bound on the expected rank of a rational elliptic curve E over an S_n-extension of $\mathbb{Q}$ for general n.

Theorem 3.48 (McKay conjecture for $p = 2$, see [46]). *Let G be a finite group and let $P \leqslant G$ be a 2-Sylow subgroup. For $H \leqslant G$, let* $\mathrm{Irr}(H)$ *denote the set of isomorphism classes of complex irreducible representations of H. Let* $\mathrm{Irr}'(H) = \{\rho \in \mathrm{Irr}(H) : 2 \nmid \dim \rho\}$. *Then*

$$| \mathrm{Irr}'(G) | = | \mathrm{Irr}'(N_G(P)) |,$$

where $N_G(P)$ is the normaliser of P in G.

Lemma 3.49 (See Exercise 4.14 in [30]). *For $n > 6$, there are precisely four representations of S_n of dimension less than n. Two of these have dimension 1 and two have dimension $n - 1$.*

Lemma 3.50. *Let P_k be the 2-Sylow subgroup of S_{2^k}. Then $P_k/[P_k, P_k] \cong C_2^k$, where $[P_k, P_k]$ denotes the commutator subgroup.*

Proof. We have $P_k = C_2^{\wr k} = C_2 \wr \cdots \wr C_2$, the wreath product with k copies of C_2 (see, e.g. [17, Example 2.6.1]), so we proceed by induction. For $k = 1$, we have $P_1 = C_2^{\wr 1} = C_2$. We assume that $P_k/[P_k, P_k] \cong C_2^k$. Now, if H is the abelianisation of G, then the abelianisation of $G \wr C_2$ is the abelianisation of $H \wr C_2$. Hence, $P_{k+1}/[P_{k+1}, P_{k+1}]$ is the abelianisation of $C_2^k \wr C_2$ which is C_2^{k+1}. □

Theorem 3.51. *Let $E/\mathbb{Q}$ be any elliptic curve with $w(E/\mathbb{Q}) = -1$ and let K be any extension of $\mathbb{Q}$ with* $\mathrm{Gal}(K/\mathbb{Q}) = S_n$. *Suppose that $(N_E, \Delta_K) = 1$. If the parity conjecture holds, then*

$$\mathrm{rk}(E/K) \geqslant \frac{n}{2}\left(\prod_k 2^{ka_k} - 2\right),$$

where $n = \sum_k a_k 2^k$ is the binary expansion of n with $a_k = 0$ or 1.

Proof. By Lemma 2.18, the parity conjecture for E over all subfields of K implies the parity conjecture for the twist of E by any irreducible self-dual representation ρ of $\mathrm{Gal}(F/\mathbb{Q})$ (the fact that all representations of S_n can be written as linear combination of permutation modules follows from [40, §6.1]). Thus, it suffices to prove that the parity conjecture for twists implies the result.

The irreducible representations of S_n are self-dual and there are two one-dimensional irreducible representations. Thus, by Theorem 3.46, to find a lower bound on the rank, it suffices to find a lower bound on the number of pairs of odd-dimensional irreducible representations of S_n.

Theorem 3.48 says that the number of odd-dimensional irreducible representations of S_n is equal to the number of one-dimensional representations of a 2-Sylow subgroup of S_n, since the normaliser of a 2-Sylow subgroup of S_n is itself and the dimension of an irreducible representation divides the order of the group. Since $n = \sum_k a_k 2^k$, the 2-Sylow subgroup of S_n is the 2-Sylow subgroup of $\prod_{k : a_k \neq 0} S_{2^k}$. By Lemma 3.50, the number of one-dimensional representations of the

2-Sylow subgroup of S_{2^k} is 2^k. Hence, the number of one-dimensional representations of the 2-Sylow subgroup of $\prod_{k:a_k\neq 0} S_{2^k}$ is $\prod_k 2^{ka_k}$. Theorem 3.48 then tells us that there are $\frac{1}{2}\prod_k 2^{ka_k}$ pairs of odd-dimensional representations of S_n.

By Lemma 3.49, for $n > 6$ other than the trivial and the sign representation, all of the odd-dimensional representations have dimension at least n, unless n is even in which case there are also two $(n-1)$-dimensional representations. Hence, assuming the parity conjecture for twists, for $n > 6$, we have

$$\mathrm{rk}(E/K) = \dim(E(K)\otimes_{\mathbb{Z}}\mathbb{C}) \geqslant \frac{n}{2}\left(\prod_k 2^{ka_k} - 2\right).$$

Using Theorem 3.46(*ii*), a simple check shows that the result is also true for $n \leqslant 6$. □

Example 3.52. Fix $E : y^2 + y = x^3 - x$ and K an S_{14}-extension of $\mathbb{Q}$ with $37 \nmid \Delta_K$. Then $w(E/\mathbb{Q}) = -1$ and $14 = 2 + 2^2 + 2^3$, so assuming the parity conjecture for twists, $\mathrm{rk}(E/K) \geqslant \frac{14}{2}\cdot(2^6 - 2) = 434$.

Remark 3.53. The bound in Theorem 3.51 is much lower than we expect the rank to be since most of the representations have dimension significantly larger than n. For example, let K be an S_7-extension of $\mathbb{Q}$ and let $E/\mathbb{Q}$ with $w(E/\mathbb{Q}) = -1$. Our bound says that $\mathrm{rk}(E/K) \geqslant 21$. However, the dimensions of the odd-dimensional irreducible representations of S_7 are 1, 1, 15, 15, 21, 21, 35 and 35. So, assuming the parity conjecture for twists, Theorem 3.46(*ii*) gives $\mathrm{rk}(E/K) \geqslant 72$.

3.16 | Heegner hypothesis

When studying Heegner points, one often imposes the *Heegner hypothesis*, that the quadratic field K is imaginary and that all primes of bad reduction of $E/\mathbb{Q}$ split in K (e.g. in Kolyvagin's work on the Birch–Swinnerton-Dyer conjecture, see [34]). From root number calculations, this ensures the odd order of vanishing of L-functions of E over K and of certain twists of E, as we now explain.

Proposition 3.54. *Let $E/\mathbb{Q}$ be an elliptic curve and let K be a quadratic extension of $\mathbb{Q}$ that satisfies the Heegner hypothesis. Let F be a C_n-extension of K and assume further that* $\mathrm{Gal}(F/\mathbb{Q}) = D_{2n}$, *the dihedral group with $2n$ elements. Assume that $(N_E, \Delta_F) = 1$. Then*

(i) *For χ any of the one-dimensional representations of* $\mathrm{Gal}(F/K)$, $\mathrm{ord}_{s=1}L(E/K,\chi,s)$ *is odd.*
(ii) *The order of vanishing of the L-function of E/F satisfies* $\mathrm{ord}_{s=1}L(E/F,s) \geqslant n$.
(iii) *Assuming the parity conjecture for twists,* $\mathrm{rk}(E/F) \geqslant n$.

Proof. Let $H = \mathrm{Gal}(F/K)$ and $G = \mathrm{Gal}(F/\mathbb{Q}) = D_{2n}$. The representations of D_{2n} are all self-dual. The one-dimensional representations are $\mathbb{1}$, the representation ϵ that factors through $\mathrm{Gal}(K/\mathbb{Q})$, and, if n is even, two more representations ϵ_1 and ϵ_2. There are $\frac{n-1}{2}$ irreducible two-dimensional representations if n is odd and $\frac{n-2}{2}$ irreducible two-dimensional representations if n is even. Call the irreducible two-dimensional representations ρ_i.

(i) By the inductivity of L-functions, for χ any of the one-dimensional representations of $\mathrm{Gal}(F/K)$,

$$L(E/K,\chi,s) = L(E/\mathbb{Q},\mathrm{Ind}_H^G\chi,s) = L(E/\mathbb{Q},\rho,s),$$

where ρ is a two-dimensional representation of D_{2n}. The determinant character of ρ is ϵ since ρ is either $\mathbb{1} \oplus \epsilon, \epsilon_1 \oplus \epsilon_2$ or ρ_i, all of which have determinant character ϵ. Hence, by the Heegner hypothesis on K and in the notation of Theorem 2.15, α_ρ is negative and satisfies $(\frac{\alpha_\rho}{N_E}) = +1$. Thus,

$$w(E/\mathbb{Q}, \rho) = (\pm 1)^2 \cdot (-1) \cdot (+1) = -1.$$

By the inductivity of root numbers (Theorem 2.16(*iii*)), $w(E/K, \chi) = -1$ and, since we know the analytic continuation of $L(E/K, \chi, s)$ and that it satisfies a functional equation whose sign is $w(E/K, \chi)$ (see, e.g. [61, Proposition 4·13]), this implies that $\mathrm{ord}_{s=1} L(E/K, \chi, s)$ is odd.

(ii) By the inductivity of L-functions,

$$L(E/F, s) = \prod_{\chi} L(E/K, \chi, s),$$

where χ runs over the one-dimensional representations of $\mathrm{Gal}(F/K)$. The result follows from part (i).

(iii) Assuming the parity conjecture for twists, $\langle \rho, E(F) \otimes_{\mathbb{Z}} \mathbb{C} \rangle \geqslant 1$ where ρ is ρ_i, $\mathbb{1} \oplus \epsilon$ or $\epsilon_1 \oplus \epsilon_2$ by the root number calculation in part (i). Hence, $\mathrm{rk}(E/F) \geqslant n$. □

3.17 | Artin representations that always appear with even multiplicity in $E(K) \otimes_{\mathbb{Z}} \mathbb{C}$

The parity conjecture for twists tells us the parity of the multiplicity of a representation ρ in $E(K) \otimes_{\mathbb{Z}} \mathbb{C}$. Conversely, if ρ is self-dual, irreducible and has Schur index 2 (e.g. ρ is symplectic), then it must appear with even multiplicity in $E(K) \otimes_{\mathbb{Z}} \mathbb{C}$. This has been checked to be compatible with root numbers in most cases, see [57, Proposition E] and [58]. On the other hand, root numbers suggest that certain representations must always appear with even multiplicity despite having Schur index 1.

Proposition 3.55 (Rohrlich [57], Proposition D). *Let K be a Galois extension of $\mathbb{Q}$ where* $\mathrm{Gal}(K/\mathbb{Q}) = D_{2q} \times D_{2r} \times D_{2s} \times D_{2t}$ *for distinct primes q, r, s, $t \geqslant 5$ and let τ be an irreducible 16-dimensional representation of* $\mathrm{Gal}(K/\mathbb{Q})$. *Then $w(E/\mathbb{Q}, \tau) = +1$ for every E over $\mathbb{Q}$.*

Proposition 3.55 tells us that, assuming the parity conjecture for twists, the multiplicity of τ in $E(K) \otimes_{\mathbb{Z}} \mathbb{C}$ is always even, which is as mysterious as the fact that every $E/\mathbb{Q}$ should have even rank over any number field which is Galois over $\mathbb{Q}$ and in which all places split into an even number of places (see Lemma 3.2).

4 | MINIMALIST CONJECTURE FOR TWISTS

There is a folklore 'minimalist conjecture', which says that, generically, the rank of an elliptic curve $E/\mathbb{Q}$ is 0 or 1 depending on whether $w(E/\mathbb{Q}) = +1$ or -1 (see, e.g. [26, Conjecture 8.2]). We propose a minimalist conjecture for Artin twists, which gives the expected Galois module structure of $E(F) \otimes_{\mathbb{Z}} \mathbb{C}$ for most elliptic curves $E/\mathbb{Q}$, where F is a finite Galois extension of $\mathbb{Q}$

(see Conjecture 4.3 and Theorems 4.7 and 4.10 below). It says that, generically, if $E/\mathbb{Q}$ is an elliptic curve and ρ is an irreducible self-dual Artin representation that factors through $F/\mathbb{Q}$, then ρ appears in $E(F) \otimes_{\mathbb{Z}} \mathbb{C}$ with multiplicity 0 or 1, depending on whether the global root number of the twist of E by ρ is $+1$ or -1.

Example 4.1. Let $E/\mathbb{Q}$ be any elliptic curve with $w(E/\mathbb{Q}) = -1$, and let F be any extension of $\mathbb{Q}$ with $\mathrm{Gal}(F/\mathbb{Q}) = A_5$ and $(N_E, \Delta_F) = 1$. By the conductor-discriminant formula, this means that N_E is coprime to the conductors of the representations of $\mathrm{Gal}(F/\mathbb{Q})$. We claim that $\mathrm{rk}(E/F) \geqslant 12$.

There are five irreducible representations of A_5 and they are all self-dual: $\mathbb{1}$, one 4-dimensional representation ρ, one 5-dimensional representation σ and two 3-dimensional representations τ_1 and τ_2. We can write

$$E(F) \otimes_{\mathbb{Z}} \mathbb{C} = \mathbb{1}^{\oplus a} \oplus \rho^{\oplus b} \oplus \sigma^{\oplus c} \oplus \tau_1^{\oplus d} \oplus \tau_2^{\oplus e}.$$

Since $\mathrm{rk}(E/F) = \dim(E(F) \otimes_{\mathbb{Z}} \mathbb{C})$,

$$\mathrm{rk}(E/F) = a + 4b + 5c + 3d + 3e.$$

We have $\det(\sigma) = \det(\tau_i) = \mathbb{1}$ since A_5 has no subgroup of index 2. Hence, by Theorem 3.46, the parity conjecture for twists implies that a, c, d and e are odd. In particular, $\mathrm{rk}(E/F) \geqslant 12$.

We typically expect to have exactly

$$E(F) \otimes_{\mathbb{Z}} \mathbb{C} = \mathbb{1} \oplus \sigma \oplus \tau_1 \oplus \tau_2,$$

and $\mathrm{rk}(E/F) = 12$. This is based on a 'minimalist conjecture for twists'. The idea is that for any elliptic curve $E/\mathbb{Q}$ and any self-dual irreducible Artin representation τ that factors through an extension $F/\mathbb{Q}$, the contribution to the rank of E/F by τ should be as small as the parity conjecture for twists will allow.

Notation 4.2. For $E/\mathbb{Q}$ an elliptic curve, it is isomorphic to a unique curve $E_{A,B} : y^2 = x^3 + Ax + B$ where $A, B \in \mathbb{Z}$ and for all primes p, either $p^4 \nmid A$ or $p^6 \nmid B$. The naive height of $E_{A,B}$ is

$$H(E_{A,B}) = \max(4|A^3|, 27B^2).$$

We say that 100% of elliptic curves over $\mathbb{Q}$ satisfy a property T if

$$\lim_{X\to\infty} \frac{\#\{E_{A,B} | H(E_{A,B}) < X \text{ and } E_{A,B} \text{ satisfies property } T\}}{\#\{E_{A,B} | H(E_{A,B}) < X\}} = 1,$$

where for all primes p, either $p^4 \nmid A$ or $p^6 \nmid B$.

Conjecture 4.3 (Minimalist conjecture for twists). *Let F be a Galois extension of $\mathbb{Q}$ and let ρ be an irreducible Artin representation that factors through $F/\mathbb{Q}$. For 100% of elliptic curves $E/\mathbb{Q}$,*

$$\langle \rho, E(F) \otimes_{\mathbb{Z}} \mathbb{C} \rangle = \begin{cases} 0 & \text{if } \rho \text{ is not self-dual,} \\ 0 & \text{if } w(E/\mathbb{Q}, \rho) = +1, \\ 1 & \text{if } w(E/\mathbb{Q}, \rho) = -1. \end{cases}$$

Since the global root number of the twist is the conjectured sign in the functional equation relating $L(E/\mathbb{Q}, \rho, s)$ and $L(E/\mathbb{Q}, \rho^*, 2-s)$, if ρ is self-dual, the parity of the order of vanishing of $L(E/\mathbb{Q}, \rho, s)$ at $s = 1$ is governed by $w(E/\mathbb{Q}, \rho)$. For most elliptic curves, one expects the order of vanishing of the twisted L-function to be as small as is allowed by the functional equation. If ρ is not self-dual, the functional equation does not tell us anything about the order of vanishing of $L(E/\mathbb{Q}, \rho, s)$ at $s = 1$. In this case, for most elliptic curves, we expect the order of vanishing to be zero and that ρ does not appear in $E(F) \otimes_{\mathbb{Z}} \mathbb{C}$.

Remark 4.4. If ρ is a complex irreducible representation with Schur index n that factors through $F/\mathbb{Q}$, the multiplicity of ρ in $E(F) \otimes_{\mathbb{Z}} \mathbb{C}$ is divisible by n. The Schur index of an irreducible self-dual character can only be 1 or 2 by the Brauer–Speiser theorem [4, 29, 66]. So, in the context of root numbers and the minimalist conjecture, Schur indices never force the multiplicity of an irreducible self-dual representation ρ in $E(F) \otimes_{\mathbb{Z}} \mathbb{C}$ to be greater than 1.

Lemma 4.5. *Let F be a Galois extension of $\mathbb{Q}$, let ρ be an irreducible Artin representation that factors through $F/\mathbb{Q}$ and let D be a non-zero integer. The minimalist conjecture for twists implies that for* 100% *of elliptic curves $E/\mathbb{Q}$ with $(N_E, D) = 1$,*

$$\langle \rho, E(F) \otimes_{\mathbb{Z}} \mathbb{C} \rangle = \begin{cases} 0 & \textit{if } \rho \textit{ is not self-dual,} \\ 0 & \textit{if } w(E/\mathbb{Q}, \rho) = +1, \\ 1 & \textit{if } w(E/\mathbb{Q}, \rho) = -1. \end{cases}$$

Proof. It is known that, for any integer D, when ordered by the height of the coefficients, there is a positive proportion of elliptic curves over $\mathbb{Q}$ whose conductor is coprime to D (see, e.g. Theorem 4.2(2) of [11]; their ordering is slightly different, which may result in a different density, but we only need to know that this density is non-zero). In other words, $\lim_{X \to \infty} \frac{\#N}{\#T} = k > 0$ where T is the set of curves $E_{A,B}$ such that $H(E_{A,B}) < X$ and $N \subset T$ is the set of elliptic curves $E_{A,B}$ such that $(N_E, D) = 1$. Let $M \subset T$ be the set of curves $E_{A,B}$ that do not satisfy the conclusion of Conjecture 4.3, so that

$$\frac{\#N \cap M}{\#N} \leqslant \frac{\#M}{\#N} = \frac{\#M}{\#T} \cdot \frac{\#T}{\#N} \to 0 \cdot \frac{1}{k} = 0 \quad \text{as} \quad X \to \infty,$$

where we have used Conjecture 4.3 for $\#M/\#T \to 0$. This proves the lemma. □

Lemma 4.6. *Let $E/\mathbb{Q}$ be an elliptic curve. Let F be a Galois extension of $\mathbb{Q}$ that does not contain any quadratic number field. For any self-dual* $\mathrm{Gal}(F/\mathbb{Q})$*-representation ρ whose conductor is coprime to N_E,*

$$w(E/\mathbb{Q}, \rho) = w(E/\mathbb{Q})^{\dim \rho}.$$

Proof. Since $\mathrm{Gal}(F/\mathbb{Q})$ has no index 2 subgroup, in the notation of Theorem 2.15, $\alpha_\rho = 1$ for any self-dual $\mathrm{Gal}(F/\mathbb{Q})$-representation ρ. So, by Theorem 2.15, $w(E/\mathbb{Q}, \rho) = w(E/\mathbb{Q})^{\dim \rho}$. □

Theorem 4.7. *Let F be a Galois extension of $\mathbb{Q}$ that does not contain any quadratic number field. Write W_G for the direct sum of the odd-dimensional irreducible self-dual representations of $G =$* $\mathrm{Gal}(F/\mathbb{Q})$ *and $k = \dim W_G$. Assuming the minimalist conjecture for twists, for* 100% *of elliptic* *curves $E/\mathbb{Q}$ with $(N_E, \Delta_F) = 1$*

$$E(F) \otimes_{\mathbb{Z}} \mathbb{C} = \begin{cases} W_G & \text{if } w(E/\mathbb{Q}) = -1, \\ 0 & \text{if } w(E/\mathbb{Q}) = +1. \end{cases}$$

In particular, for 100% of elliptic curves $E/\mathbb{Q}$ with $(N_E, \Delta_F) = 1$,

$$\mathrm{rk}(E/F) = \begin{cases} k & \text{if } w(E/\mathbb{Q}) = -1, \\ 0 & \text{if } w(E/\mathbb{Q}) = +1. \end{cases}$$

Proof. Let ρ be a representation of $\mathrm{Gal}(F/\mathbb{Q})$. By the conductor-discriminant formula, this ensures that the conductor of ρ is coprime to N_E. If ρ is not self-dual, by Lemma 4.5, the minimalist conjecture for twists implies that ρ does not appear in $E(F) \otimes_{\mathbb{Z}} \mathbb{C}$ for 100% of elliptic curves $E/\mathbb{Q}$ with $(N_E, \Delta_F) = 1$. If ρ is self-dual, since $\mathrm{Gal}(F/\mathbb{Q})$ has no index 2 subgroup, by Lemma 4.6, $w(E/\mathbb{Q}, \rho) = w(E/\mathbb{Q})^{\dim \rho}$ for $E/\mathbb{Q}$ any elliptic curve with $(N_E, \Delta_F) = 1$. By Lemma 4.5, the minimalist conjecture for twists implies that, for 100% of elliptic curves $E/\mathbb{Q}$ with $(N_E, \Delta_F) = 1$,

$$\langle \rho, E(F) \otimes_{\mathbb{Z}} \mathbb{C} \rangle = \begin{cases} 1 & \text{if } \rho \text{ has odd dimension and } w(E/\mathbb{Q}, \rho) = -1, \\ 0 & \text{otherwise,} \end{cases}$$

which gives us the result. □

Remark 4.8. Theorem 4.7 says that elliptic curves of rank 1 over $\mathbb{Q}$ tend to gain many points over Galois extensions with no quadratic subfields, while elliptic curves of rank 0 over $\mathbb{Q}$ tend not to obtain any new points. It suggests that the equation $y^2 + y = x^3 - x$ is 'easy to solve', whereas the equation $y^2 + y = x^3 - x^2$ is 'hard to solve' over most Galois extensions of $\mathbb{Q}$ with no quadratic subfield.

Remark 4.9. In the setting of Theorem 4.7, we expect even-dimensional irreducible Artin representations to be very rare inside Mordell–Weil groups.

Theorem 4.10. *Let F be a Galois extension of $\mathbb{Q}$. Assuming the minimalist conjecture for twists, for 100% of $E/\mathbb{Q}$ with $(N_E, 2\Delta_F) = 1$, the Galois module $E(F) \otimes_{\mathbb{Z}} \mathbb{C}$ depends only on $N_E \pmod{8\Delta_F}$ and $w(E/\mathbb{Q})$.*

Proof. By Lemma 4.5, it is enough to show that $w(E/\mathbb{Q}, \rho)$ only depends on $N_E \pmod{8\Delta_F}$ and $w(E/\mathbb{Q})$ for every self-dual representation ρ of $\mathrm{Gal}(F/\mathbb{Q})$. Let ρ be any self-dual representation of $\mathrm{Gal}(F/\mathbb{Q})$ and suppose that we have E and E' elliptic curves over $\mathbb{Q}$ with $N_E \equiv N_{E'} \pmod{8\Delta_F}$, $(N_E, 2\Delta_F) = 1 = (N_{E'}, 2\Delta_F)$ and $w(E/\mathbb{Q}) = w(E'/\mathbb{Q})$. By the conductor-discriminant formula, this ensures that N_E and $N_{E'}$ are coprime to the conductor of ρ, so we can apply Theorem 2.15 to calculate $w(E/\mathbb{Q}, \rho)$. In the notation of Theorem 2.15, $\alpha_\rho \mid \Delta_F$. Since $N_E \equiv N_{E'} \pmod{8\alpha_\rho}$ and N_E and $N_{E'}$ are odd, by quadratic reciprocity, we have $(\frac{\alpha_\rho}{N_E}) = (\frac{\alpha_\rho}{N_{E'}})$. Hence, by Theorem 2.15, $w(E/\mathbb{Q}, \rho) = w(E'/\mathbb{Q}, \rho)$. □

Example 4.11. Let F be the splitting field of the polynomial

$$x^{10} + 5x^8 + 15x^6 + 20x^4 + 25x^2 + 15.$$

Then, $\mathrm{Gal}(F/\mathbb{Q}) = D_{10}$ and $\Delta_F = -3^5 \cdot 5^{13}$. Theorem 4.10 tells us that, for 100% of elliptic curves $E/\mathbb{Q}$ with $(N_E, 2\Delta_F) = 1$, the Galois module structure of $E(F) \otimes_{\mathbb{Z}} \mathbb{Q}$ depends on N_E modulo $8 \cdot 3^5 \cdot 5^{13}$ and $w(E/\mathbb{Q})$. In fact, we will show that it only depends on $N_E \pmod{15}$ and $w(E/\mathbb{Q})$.

The representations of $\mathrm{Gal}(F/\mathbb{Q})$ are the trivial representation $\mathbb{1}$, one 1-dimensional representation ϵ that factors through $\mathbb{Q}(\sqrt{-15})$ and two 2-dimensional representations ρ_1 and ρ_2, both of which have determinant ϵ. Thus, when $(N_E, 2\Delta_F) = 1$, by Theorem 2.15,

$$w(E/\mathbb{Q}, \epsilon) = \begin{cases} -w(E/\mathbb{Q}) & \text{if } \left(\frac{-15}{N_E}\right) = +1, \\ w(E/\mathbb{Q}) & \text{if } \left(\frac{-15}{N_E}\right) = -1, \end{cases} \qquad w(E/\mathbb{Q}, \rho_i) = \begin{cases} -1 & \text{if } \left(\frac{-15}{N_E}\right) = +1, \\ +1 & \text{if } \left(\frac{-15}{N_E}\right) = -1. \end{cases}$$

We have

$$\left(\frac{-15}{N_E}\right) = \begin{cases} +1 & \text{if } N_E \equiv 1,\ 2,\ 4 \text{ or } 8 \pmod{15}; \\ -1 & \text{if } N_E \equiv 7,\ 11,\ 13 \text{ or } 14 \pmod{15}. \end{cases}$$

Note that when $(N_E, 2\Delta_F) = 1$, these congruence classes are the only possibilities for N_E modulo 15. Hence, assuming the minimalist conjecture for twists, for 100% of elliptic curves $E/\mathbb{Q}$ with $(N_E, 2\Delta_F) = 1$

$$E(F) \otimes_{\mathbb{Z}} \mathbb{C} = \begin{cases} \epsilon \oplus \rho_1 \oplus \rho_2 & \text{if } N_E \equiv 1,\ 2,\ 4 \text{ or } 8 \pmod{15} \text{ and } w(E/\mathbb{Q}) = +1; \\ \mathbb{1} \oplus \rho_1 \oplus \rho_2 & \text{if } N_E \equiv 1,\ 2,\ 4 \text{ or } 8 \pmod{15} \text{ and } w(E/\mathbb{Q}) = -1; \\ 0 & \text{if } N_E \equiv 7,\ 11,\ 13 \text{ or } 14 \pmod{15} \text{ and } w(E/\mathbb{Q}) = +1; \\ \mathbb{1} \oplus \epsilon & \text{if } N_E \equiv 7,\ 11,\ 13 \text{ or } 14 \pmod{15} \text{ and } w(E/\mathbb{Q}) = -1. \end{cases}$$

APPENDIX A: LOCAL ROOT NUMBERS OF ELLIPTIC CURVES OVER $\mathbb{Q}_2$

The following table can be used to calculate $w(E/\mathbb{Q}_2)$, including when $E/\mathbb{Q}_2$ has additive reduction. It is based on Table III in [54], which generalises results of Halberstadt [36] to non-minimal Weierstrass equations. For a discussion on what can be done to calculate root numbers over extensions of $\mathbb{Q}_2$, see §2.2.

Notation A.1. Let $E/\mathbb{Q}_2$ be an elliptic curve given by a Weierstrass equation.

- Let $m = \min\{\lfloor v_2(\Delta_E)/12 \rfloor, \lfloor v_2(c_6)/6 \rfloor, \lfloor v_2(c_4)/4 \rfloor\}$. Define

$$(C_\Delta, C_6, C_4) = (v_2(\Delta_E) - 12m, v_2(c_6) - 6m, v_2(c_4) - 4m).$$

  In other words, take $(v_2(\Delta_E), v_2(c_6), v_2(c_4))$ and subtract multiples of (12,6,4) entry-wise until reaching the smallest triple of non-negative integers (C_Δ, C_6, C_4). By convention, $v_2(0) = \infty$.
- $x' = x/2^{v_2(x)}$.
- $c_{6,e} = c_6/2^{v_2(c_6) - C_6 + e}$; if $c_6 = 0$, then $c_{6,e} = 0$.

Example A.2. If $E : y^2 = x^3 - 64x - 128$, then $\Delta_E = 2^{18} \cdot 37$, $c_6 = 2^{12} \cdot 3$ and $c_4 = 2^{10} \cdot 3$ so $(C_\Delta, C_6, C_4) = (6, 6, 6)$. We have $c_6' = 3$ and the table below tells us that $w(E/\mathbb{Q}_2) = -1$.

C_Δ	C_6	C_4	Extra conditions	$w(E/\mathbb{Q}_2)$
0	0	0	$c_6' \equiv 3 \pmod 4$	+1
$\geqslant 0$	0	0	$c_6' \equiv 1 \pmod 4$	−1
0	3	3	$c_4' \equiv 1 \pmod 4$ and $c_6' \equiv \pm 1 \pmod 8$ or $c_4' \equiv 3 \pmod 4$ and $c_6' \equiv 1$ or $3 \pmod 8$	+1
0	3	3	$c_4' \equiv 1 \pmod 4$ and $c_6' \equiv 3$ or $5 \pmod 8$ or $c_4' \equiv 3 \pmod 4$ and $c_6' \equiv 5$ or $7 \pmod 8$	−1
0	3	$\geqslant 4$	$c_6' \equiv 1 \pmod 4$	+1
0	3	$\geqslant 4$	$c_6' \equiv 3 \pmod 4$	−1
0	4	2	$c_4' \equiv 1 \pmod 4$ and $c_4' + 4c_6' \equiv 9$ or $13 \pmod{16}$	+1
0	4	2	$c_4' \equiv 1 \pmod 4$ and $c_4' + 4c_6' \not\equiv 9$ or $13 \pmod{16}$	−1
0	$\geqslant 4$	2	$c_4' \equiv 3 \pmod 4$ and $C_6 = 4$	+1
0	$\geqslant 4$	2	$c_4' \equiv 3 \pmod 4$ and $C_6 \neq 4$	−1
0	5	2	$c_4' \equiv 1 \pmod 4$ and $c_4' + 4c_{6,4} \equiv 5$ or $9 \pmod{16}$	−1
0	5	2	$c_4' \equiv 1 \pmod 4$ and $c_4' + 4c_{6,4} \not\equiv 5$ or $9 \pmod{16}$	+1
0	$\geqslant 6$	2	$c_4' \equiv 1 \pmod 4$ and $c_4' + 4c_{6,4} \equiv 5$ or $9 \pmod{16}$	+1
0	$\geqslant 6$	2	$c_4' \equiv 1 \pmod 4$ and $c_4' + 4c_{6,4} \not\equiv 5$ or $9 \pmod{16}$	−1
$\geqslant 1$	0	0	$c_6' \equiv 3 \pmod 4$ and $c_6' \equiv 3 \pmod 8$	+1
$\geqslant 1$	0	0	$c_6' \equiv 3 \pmod 4$ and $c_6' \not\equiv 3 \pmod 8$	−1
1	3	2	$c_4' + 4c_6' \equiv 3 \pmod{16}$ or $c_4' \equiv 11 \pmod{16}$	+1
1	3	2	$c_4' + 4c_6' \not\equiv 3 \pmod{16}$ and $c_4' \not\equiv 11 \pmod{16}$	−1
2	3	2	$\Delta_E' \equiv c_6' \pmod 4$	+1
2	3	2	$\Delta_E' \not\equiv c_6' \pmod 4$	−1
2	4	3	$c_4' + c_6' \equiv 0$ or $6 \pmod 8$	+1
2	4	3	$c_4' + c_6' \not\equiv 0$ or $6 \pmod 8$	−1
2	4	$\geqslant 4$	$c_6' \equiv 1 \pmod 4$	+1
2	4	$\geqslant 4$	$c_6' \not\equiv 1 \pmod 4$	−1
3	3	2	$\Delta_E' \equiv 3 \pmod 4$	+1
3	3	2	$\Delta_E' \not\equiv 3 \pmod 4$	−1
3	5	3	$2c_6' + c_4' \equiv 1$ or $3 \pmod 8$	+1
3	5	3	$2c_6' + c_4' \equiv 5$ or $7 \pmod 8$	−1
3	$\geqslant 6$	3	$c_4' \equiv 5$ or $7 \pmod 8$	+1
3	$\geqslant 6$	3	$c_4' \equiv 1$ or $3 \pmod 8$	−1
$\geqslant 4$	3	2	$c_6' \equiv 3 \pmod 4$	+1
$\geqslant 4$	3	2	$c_6' \not\equiv 3 \pmod 4$	−1
4	5	4	$c_4' \equiv c_6' \pmod 4$ and $c_4' \equiv 1 \pmod 4$	+1
4	5	4	$c_4' \equiv c_6' \pmod 4$ and $c_4' \equiv 3 \pmod 4$	−1
4	5	4	$c_4' \equiv 1 \equiv -c_6' \pmod 4$ and $c_4'c_6' \equiv 3 \pmod 8$	+1
4	5	4	$c_4' \equiv 1 \equiv -c_6' \pmod 4$ and $c_4'c_6' \not\equiv 3 \pmod 8$	−1
4	5	4	$c_6' \equiv 1 \equiv -c_4' \pmod 4$	−1
4	5	5	$c_6' \equiv 1 \pmod 4$ and $c_6' \equiv 5 \pmod 8$	+1
4	5	5	$c_6' \equiv 1 \pmod 4$ and $c_6' \equiv 1 \pmod 8$	−1
4	5	$\geqslant 5$	$c_6' \equiv 3 \pmod 4$ and $C_4 = 5$	+1

(Continues)

C_Δ	C_6	C_4	Extra conditions	$w(E/\mathbb{Q}_2)$
4	5	$\geqslant 5$	$c_6' \equiv 3 \pmod 4$ and $C_4 \neq 5$	-1
4	5	$\geqslant 6$	$c_6' \equiv 1 \pmod 4$	-1
6	6	5	$c_4' \equiv 3 \pmod 4$	$+1$
6	6	5	$c_4' \equiv 1 \pmod 4$	-1
6	6	$\geqslant 6$	$c_6' \equiv 1 \pmod 4$;	$+1$
6	6	$\geqslant 6$	$c_6' \equiv 3 \pmod 4$;	-1
6	$\geqslant 7$	4	$c_4' \equiv 1 \pmod 4$ and $C_6 = 7$	$+1$
6	$\geqslant 7$	4	$c_4' \equiv 1 \pmod 4$ and $C_6 \neq 7$	-1
6	$\geqslant 7$	4	$c_4' \equiv 3 \pmod 4$ and $c_4' - 4c_{6,7} \equiv 7$ or $11 \pmod{16}$	$+1$
6	$\geqslant 7$	4	$c_4' \equiv 3 \pmod 4$ and $c_4' - 4c_{6,7} \not\equiv 7$ or $11 \pmod{16}$	-1
7	6	4	$c_6' \equiv 5$ or $5c_4' \pmod 8$	$+1$
7	6	4	$c_6' \not\equiv 5$ or $5c_4' \pmod 8$	-1
8	6	4	$2c_6' + c_4' \equiv 3 \pmod{16}$	$+1$
8	6	4	$2c_6' + c_4' \equiv 15 \pmod{16}$	-1
8	6	4	$2c_6' + c_4' \equiv 23 \pmod{32}$	$+1$
8	6	4	$2c_6' + c_4' \equiv 7 \pmod{32}$	-1
8	6	4	$2c_6' + c_4' \equiv 11 \pmod{16}$	-1
8	7	5	$2c_4' + c_6' \equiv 7 \pmod 8$ or $c_6' \equiv 3 \pmod 8$	$+1$
8	7	5	$2c_4' + c_6' \not\equiv 7 \pmod 8$ and $c_6' \not\equiv 3 \pmod 8$	-1
8	7	6	$c_6' \equiv 1 \pmod 4$ and $2c_4' + c_6' \equiv 3 \pmod 8$	$+1$
8	7	6	$c_6' \equiv 1 \pmod 4$ and $2c_4' + c_6' \not\equiv 3 \pmod 8$	-1
8	7	$\geqslant 6$	$c_6' \equiv 3 \pmod 4$ and $C_4 = 6$	$+1$
8	7	$\geqslant 6$	$c_6' \equiv 3 \pmod 4$ and $C_4 \neq 6$	-1
8	7	$\geqslant 7$	$c_6' \equiv 1 \pmod 4$	-1
9	6	4	$2c_6' + c_4' \equiv 11 \pmod{32}$ or $c_6' \equiv 7 \pmod 8$	$+1$
9	6	4	$2c_6' + c_4' \not\equiv 11 \pmod{32}$ and $c_6' \not\equiv 7 \pmod 8$	-1
9	8	5	$2c_6' + c_4' \equiv \pm 1 \pmod 8$	$+1$
9	8	5	$2c_6' + c_4' \equiv 3$ or $5 \pmod 8$	-1
9	$\geqslant 9$	5	$c_4' \equiv 1$ or $3 \pmod 8$	$+1$
9	$\geqslant 9$	5	$c_4' \equiv 5$ or $7 \pmod 8$	-1
10	6	4	$c_6' \equiv 1 \pmod 4$	$+1$
10	6	4	$c_6' \equiv 3 \pmod 4$ and $c_4' - 2c_6' \equiv 3$ or $19 \pmod{64}$	$+1$
10	6	4	$c_6' \equiv 3 \pmod 4$ and $c_4' - 2c_6' \not\equiv 3$ or $19 \pmod{64}$	-1
10	8	6	$c_4'c_6' \equiv 3 \pmod 4$	$+1$
10	8	6	$c_4'c_6' \equiv 1 \pmod 4$	-1
10	8	$\geqslant 7$	$c_6' \equiv 1 \pmod 4$	$+1$
10	8	$\geqslant 7$	$c_6' \equiv 3 \pmod 4$	-1
11	6	4	$c_6' \equiv 1 \pmod 4$	$+1$
11	6	4	$c_6' \equiv 3 \pmod 4$ and $c_6' \equiv 3 \pmod 8$	$+1$
11	6	4	$c_6' \equiv 3 \pmod 4$ and $c_6' \equiv 7 \pmod 8$	-1

There appear to be a couple of typos in Table III of [54]: it shows $(>0,0,0)$ instead of $(\geqslant 0,0,0)$ and the definition of $c_{6,e}$ is not consistent with Halberstadt's definition. We have checked that all possible cases for (C_Δ, C_6, C_4) are covered by the table, using the equation $1728\Delta_E = c_4^3 - c_6^2$. We have also numerically checked that the table is consistent with the implementation in Magma [3] of Halberstadt's table in [36] for over one million curves (including examples from each entry).

ACKNOWLEDGEMENTS

The authors would like to thank James Bell, Kestutis Česnavičius, John Cremona, Julie Desjardins, Tim Dokchitser, Benedict Gross, Zev Klagsbrun, Chao Li, Rachel Newton, Ariel Pacetti, Ross Paterson, Ottavio Rizzo, David Rohrlich, Mohammad Sadek and Alexei Skorobogatov for useful discussions and comments. The second author is very grateful to the late John Coates for his interest, encouragement and discussions on the topic of explicit arithmetic phenomena of elliptic curves.

The first author was supported by the Engineering and Physical Sciences Research Council [EP/S021590/1], the EPSRC Centre for Doctoral Training in Geometry and Number Theory (The London School of Geometry and Number Theory) and University College London. The second author was supported by a Royal Society University Research Fellowship.

JOURNAL INFORMATION

The *Bulletin of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

REFERENCES

1. M. Bhargava and A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. **181** (2015), no. 2, 587–621.
2. M. Bisatt, *Explicit root numbers of abelian varieties*, Trans. Amer. Math. Soc. **372** (2019), 7889–7920.
3. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I: The user language*, J. Symb. Comput. **24** (1997), no. 3–4, 235–265.
4. R. Brauer, *Über Zusammenhange zwischen arithmetischen und invariantentheoretischen Eigenschaften von Gruppen linearer Substitutionen*, Sitzber. Preuss. Akad. Wiss. (1926), 410–416.
5. J. W. S. Cassels, *Arithmetic on curves of genus 1, III, The Tate–Šafarevič and Selmer groups*, Proc. London Math. Soc. **12** (1962), 259–296.
6. J. W. S. Cassels and A. Schinzel, *Selmer's conjecture and families of elliptic curves*, Bull. London Math. Soc. **14** (1982), no. 4, 345–348.
7. K. Česnavičius, *The p-parity conjecture for elliptic curves with a p-isogeny*, J. Reine Angew. Math. **719** (2016), 45–73.
8. J. Coates, T. Fukaya, K. Kato, and R. Sujatha, *Root numbers, Selmer groups and non-commutative Iwasawa theory*, J. Algebraic Geom. **19** (2010), 19–97.
9. I. Connell, *Calculating root numbers of elliptic curves over Q*, Manuscripta Math. **82** (1994), 93–104.
10. B. Conrad, K. Conrad, and H. Helfgott, *Root numbers and ranks in positive characteristic*, Adv. Math. **198** (2005), no. 2, 684–731.
11. J. E. Cremona and M. Sadek, *Local and global densities for Weierstrass models of elliptic curves*, arXiv:2003.08454.
12. H. Darmon and Y. Tian, *Heegner points over towers of Kummer extensions*, Canad. J. Math. **62** (2010), no. 5, 1060–1081.

13. C. Delaunay and C. Wüthrich, *Self-points on elliptic curves of prime conductor*, Int. J. Number Theory **5** (2009), 1–22.
14. P. Deligne, *Les constantes des équations fonctionnelles*, Seminaire Delange–Pisot–Poitou (Théorie des Nombres) 11e année, 1969/70, no 19 bis, Secrétariat Mathématique, Paris, 1970.
15. J. Desjardins, *On the variation of the root number in families of elliptic curves*, J. London Math. Soc. **99** (2018), no. 2, 1–33.
16. J. Desjardins, *Root numbers of twists of elliptic curves*, J. Théor. Nombres Bordeaux, Tome **32** (2020), no. 1, 73–101.
17. J. D. Dixon and B. Mortimer, *Permutation groups*, GTM, vol. 163, Springer, New York, 1996.
18. T. Dokchitser, *Ranks of elliptic curves in cubic extensions*, Acta Arith. **126** (2007), 357–360.
19. T. Dokchitser and V. Dokchitser, *Parity of ranks for elliptic curves with a cyclic isogeny*, J. Number Theory **128** (2008), 662–679.
20. T. Dokchitser and V. Dokchitser, *Root numbers of elliptic curves in residue characteristic 2*, Bull. London Math. Soc. **40** (2008), 516–524.
21. T. Dokchitser and V. Dokchitser, *Elliptic curves with all quadratic twists of positive rank*, Acta Arith. **137** (2009), 193–197.
22. T. Dokchitser and V. Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. Reine Angew. Math. **658** (2011), 39–64.
23. T. Dokchitser and V. Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math. **178** (2009), no. 1, 23–71.
24. T. Dokchitser and V. Dokchitser, *On the Birch–Swinnerton-Dyer quotients modulo squares*, Ann. of Math. **172** (2010), no. 1, 567–596.
25. T. Dokchitser and V. Dokchitser, *A note on the Mordell–Weil rank modulo n*, J. Number Theory **131** (2011), 1833–1839.
26. T. Dokchitser, *Notes on the parity conjecture*, Elliptic Curves, Hilbert Modular Forms and Galois Deformations, Advanced Courses in Mathematics - CRM Barcelona. Birkhäuser, Basel, 2013.
27. V. Dokchitser, *Root numbers of non-abelian twists of elliptic curves, with an appendix by T. Fisher*, Proc. London Math. Soc. (3) **91** (2005), 300–324.
28. V. Dokchitser and C. Maistret, *Parity conjecture for abelian surfaces*, Proc. London Math. Soc. **127** (2023), no. 3, 295–365.
29. B. Fein, *A note on the Brauer–Speiser theorem*, Proc. Amer. Math. Soc. **25** (1970), 620–621.
30. W. Fulton and J. Harris, *Representation theory*, GTM, vol. 129, Springer, New York, NY, 2004.
31. D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Springer Lect. Notes, vol. 751, Springer, Berlin, 1979, pp. 108–118.
32. H. Green and C. Maistret, *The 2-parity conjecture for elliptic curves with isomorphic 2-torsion*, Proc. R. Soc. A **478**, 20220112.
33. B. Gross, *Heegner points on $X_0(N)$*, Modular forms (Durham, 1983), Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., Horwood, Chichester, 1984, pp. 87–105.
34. B. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), London Math. Soc. Lecture Note Ser., vol. 153, Cambridge University Press, Cambridge, 1991, pp. 235–256.
35. B. Gross, *Some remarks on signs in functional equations*, Ramanujan J. **7** (2003), no. 1–3, 91–93.
36. E. Halberstadt, *Signes locaux des courbes elliptiques en 2 et 3*, C. R. Acad. Sci. Paris Série I Math. **326** (1998), no. 9, 1047–1052.
37. K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. **56** (1952), 227–253.
38. H. A. Helfgott, *On the behaviour of root numbers in families of elliptic curves*, arXiv: math/0408141v3.
39. P. Humphries and B. Michels, *The density of square-free integers satisfying a congruence relation*, URL (version: 2017-01-12): https://math.stackexchange.com/q/2093697.
40. G. D. James, *The representation theory of the symmetric groups*, LNM, vol. 682, Springer, Berlin, 1978.
41. B. D. Kim, *The parity theorem of elliptic curves at primes with supersingular reduction*, Compos. Math. **143** (2007), 47–72.
42. Z. Klagsbrun, B. Mazur, and K. Rubin, *Disparity in Selmer ranks of quadratic twists of elliptic curves*, Ann. of Math. **178** (2013), 287–320.
43. Z. Klagsbrun, B. Mazur, and K. Rubin, *Erratum to "Disparity in Selmer ranks of quadratic twists of elliptic curves"*, Preprint, 2022.

44. S. Kobayashi, *The local root number of elliptic curves with wild ramification*, Math. Ann. **323** (2002), 609–623.
45. D. Kriz, *Supersingular main conjectures, Sylvester's conjecture and Goldfeld's conjecture*, arXiv:2002.04767.
46. G. Malle and B. Späth, *Characters of odd degree*, Ann. of Math. **184** (2016), no. 3, 869–908.
47. B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575.
48. P. Monsky, *Generalizing the Birch–Stephens theorem. I. Modular curves*, Math. Z. **221** (1996), 415–420.
49. A. Morgan, *2-Selmer parity for hyperelliptic curves in quadratic extensions*, arXiv: 1504.01960.
50. J. Nekovář, *Selmer complexes*, Astérisque **310** (2006).
51. J. Nekovář, *On the parity of ranks of Selmer groups IV, with an appendix by J.-P. Wintenberger*, Compos. Math. **145** (2009), 1351–1359.
52. J. Nekovář, *Some consequences of a formula of Mazur and Rubin for arithmetic local constants*, Algebra Number Theory **7** (2013), no. 5, 1101–1120.
53. J. Nekovář, *Compatibility of arithmetic and algebraic local constants (the case $l \neq p$)*, Compos. Math. **151** (2015), no. 9, 1626–1646.
54. O. G. Rizzo, *Average root numbers for a nonconstant family of elliptic curves*, Compos. Math. **136** (2003), no. 1, 1–23.
55. D. E. Rohrlich, *Elliptic curves and the Weil-Deligne group*, Elliptic Curves and Related Topics, CRM Proceedings & Lecture Notes, vol. 4, American Mathematical Society, Providence, RI, 1994, pp. 125–157.
56. D. E. Rohrlich, *Variation of the root number in families of elliptic curves*, Compos. Math. **87** (1993), no. 2, 119–151.
57. D. E. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Compos. Math. **100** (1996), 311–349.
58. M. Sabitova, *Root numbers of abelian varieties*, Trans. Amer. Math. Soc. **359** (2007), no. 9, 4259–4284.
59. R. Schmidt, *Some remarks on local newforms for GL(2)*, J. Ramanujan Math. Soc. **17** (2002), no. 2, 115–147.
60. E. Selmer, *A conjecture concerning rational points on cubic curves*, Math. Scand. **2** (1954), no. 1, 49–54.
61. G. Shimura, *The special values of the zeta functions associated with Hilbert modular forms*, Duke Math. J. **45** (1978), no. 3, 637–679.
62. J. H. Silverman, *The arithmetic of elliptic vurves*, GTM, vol. 106, Springer, New York, NY, 1986.
63. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, GTM, vol. 151, Springer, New York, NY, 1994.
64. A. Skorobogatov and P. Swinnerton-Dyer, *2-Descent on elliptic curves and rational points on certain Kummer surfaces*, Adv. Math. **198** (2005), no. 2, 448–483.
65. A. Smith, *The congruent numbers have positive natural density*, arXiv:1603.08479.
66. A. Speiser, *Zahlentheoretische Sätze aus der Gruppentheorie*, Math. Z. **5** (1919), 1–6.
67. N. M. Stephens, *Congruence properties of congruent numbers*, Bull. London Math. Soc. **7** (1975), no. 2, 182–184.
68. J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable IV, vol. 476, Lecture Notes in Mathematics, Springer, Berlin, 1975, pp. 33–52.
69. J. Tate, *Number theoretic background*, Automorphic forms, representations, and L-functions (Proc. Symp. Pure Math.), vol. 33, American Mathematical Society, Providence, RI, 1979, pp. 3–26.
70. Y. Tian, *Congruent numbers and Heegner points*, Cambridge J. Math. **2** (2014), no. 1, 117–161.
71. J. Tunnell, *A classical Diophantine problem and modular forms of weight 3/2*, Invent. Math. **72** (1983), no. 2, 323–334.
72. L. C. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. **48** (1987), no. 177, 371–384.
73. C. Wuthrich, *Self-points on elliptic curves*, Algebra Number Theory **3** (2009), 283–315.