ESSENTIAL NUMBER THEORY

The Heegner–Stark theorem and Stark–Heegner points

Elias Caeiro and Henri Darmon

2025

vol. 4 no. 1

msp

Essential Number Theory
Vol. 4, No. 1, 2025
https://doi.org/10.2140/ent.2025.4.67

The Heegner–Stark theorem and Stark–Heegner points

Elias Caeiro and Henri Darmon

The determination by Heegner, Baker and Stark of the complete list of imaginary quadratic orders of class number one relies critically on the theory of complex multiplication. A conjectural extension of this theory to real quadratic fields based on the notion of rigid analytic elliptic cocycles is shown to yield similar lists for some explicit families of real quadratic orders with small regulators.

Notation 67
Introduction 68
1. Splitting of small primes in real quadratic fields 72
2. Modular parametrisations and elliptic cocycles 73
3. Stark–Heegner points 76
4. Rigid analytic period functions 79
5. Rational period functions 83
6. Yokoi's conjecture 87
7. Chowla's conjecture 91
Appendix: Computer code 95
References 97

Notation

Given $D \equiv 0, 1 \pmod 4$, let $\mathcal{O}_D = \mathbb{Z}\left[\frac{1}{2}(D + \sqrt{D})\right]$ be the unique quadratic order of discriminant D, let $\mathrm{Cl}(D)$ denote its class group in the wide sense, and let $h(D) := \#\mathrm{Cl}(D)$ denote the class number of $\mathcal{O}_D$. The discriminant D is said to be *fundamental* if $\mathcal{O}_D$ is a maximal order. If D is of the form $D_0 m^2$ with D_0 fundamental, then $\mathcal{O}_D$ is also referred to as the *order of conductor* m in $\mathcal{O}_{D_0}$.

Class field theory associates to D an abelian extension H_D of $K_D := \mathbb{Q}(\sqrt{D})$, the *ring class field of the order* $\mathcal{O}_D$, whose Galois group $\mathrm{Gal}(H_D/K_D)$ is isomorphic to $\mathrm{Cl}(D)$.

Let χ_D be the quadratic Dirichlet character of conductor D attached to K_D, and let $L(s, \chi_D)$ be the associated Dirichlet L-series.

MSC2020: 11R11, 11R42.
Keywords: class number one problem, real quadratic fields, Stark–Heegner points, rigid analytic cocycles.

© 2025 The Authors, under license to MSP (Mathematical Sciences Publishers).

When D is positive, let $\varepsilon_D > 1$ denote the fundamental unit of $\mathcal{O}_D$. It has norm -1 when the wide and narrow class numbers agree, and norm 1 otherwise. The quantity $\log|\varepsilon_D|$ is called the *regulator* of $\mathcal{O}_D$.

If E is an elliptic curve over $\mathbb{Q}$, let $E^{(D)}$ denote its D-th quadratic twist.

Introduction

The Heegner–Stark theorem of the title is the celebrated result that there are precisely 13 negative discriminants D for which $h(D) = 1$, namely,

$$D = -3,\ -4,\ -7,\ -8,\ -11,\ -12,\ -16,\ -19,\ -27,\ -28,\ -43,\ -67,\ -163. \quad (1)$$

It was originally conjectured in a slightly different form by Gauss in his *Disquisitiones Arithmeticae*; see [18]. Heegner's original proof [20] exploits the theory of complex multiplication to show that the negative discriminants of class number one give rise to integral points on an affine "nonsplit Cartan" modular curve of level 24, reducing their classification to the tractable Diophantine problem of finding the integral points on a specific elliptic curve. The method is now the object of an extensive literature. Stark's work [33; 34] vindicating Heegner's approach was immediately preceded by a proof by Baker [1] exploiting linear forms in logarithms. Variants involving modular curves of levels 15, 7, 9, 11, 13 and 17 have also been described in [32], [21], [4], [29], [2] and [3] respectively. See [30, Appendix] for a general survey.

The Diophantine approach initiated by Heegner is somewhat superseded by analytic techniques based on Dirichlet's class number formula, which for $D < 0$ asserts that

$$L(1, \chi_D) = \frac{2\pi h(D)}{w\sqrt{|D|}}, \quad w := \#\mathcal{O}_D^\times. \quad (2)$$

Siegel showed that $L(1, \chi_D) \gg |D|^{-\epsilon}$ for all $\epsilon > 0$, and hence that $h(D)$ grows like $|D|^{1/2-\epsilon}$, but this result suffers from the fact that the implied constant in the lower bound cannot be effectively computed owing to the possible existence of Siegel zeroes of Dirichlet L-functions.

An important result of Goldfeld [17; 18] parlays a Hasse–Weil L-function of an elliptic curve of conductor N with a zero of order ϱ at the central point for the functional equation into an *effective* lower bound of the form

$$L(1, \chi_D) \gg \frac{\log(|D|)^{\varrho-2-\epsilon}}{\sqrt{|D|}} \quad (3)$$

for any $\epsilon > 0$, provided $\chi_D(-N) = (-1)^{\varrho-1}$. When combined with (2), this inequality leads to the lower bound $h(D) \gg \log(|D|)^{\varrho-2-\epsilon}$ with an explicit implied constant, making it possible in principle to enumerate all the quadratic imaginary orders of a given class number. The theory of complex multiplication makes a

crucial cameo appearance in Goldfeld's attack via the theorem of Gross–Zagier, which exploits Heegner points to produce the desired Hasse–Weil L-series with a zero of order $\varrho \geq 3$ at the center. A survey of the Goldfeld–Gross–Zagier solution to the effective class number problem for quadratic imaginary fields can be found in the Bourbaki seminar article by Oesterlé [28].

For positive discriminants, the analytic class number formula

$$L(1, \chi_D) = \frac{h(D)\log(\varepsilon_D)}{\sqrt{D}} \tag{4}$$

only yields asymptotic lower bounds on the product of the class number and the regulator. It is expected that there are infinitely many $D > 0$ for which $h(D) = 1$, reflecting the unproved yet widely believed fact that $\log(\varepsilon_D)$ can often be roughly as large as $|D|^{1/2}$. Proving that $h(D) = 1$ infinitely often is perhaps the most important open problem about class numbers of real quadratic fields.

The analytic class number formula nonetheless suggests that families of real quadratic orders with small fundamental units, whose regulators grow like $\log(D)$, should behave like imaginary quadratic orders. This is the case for discriminants of the form $D = n^2 \pm 4$, where $\mathcal{O}_D$ contains the explicit unit $(n + \sqrt{D})/2$. Yokoi [36] conjectured that there are exactly ten discriminants of the form $D = n^2 + 4$ with class number one, namely,

$$D = 5,\ 8,\ 13,\ 20,\ 29,\ 53,\ 68,\ 125,\ 173,\ 293. \tag{5}$$

Mollin [26] likewise predicted that there are ten class number one discriminants,

$$D = -4,\ -3,\ 5,\ 12,\ 21,\ 32,\ 45,\ 77,\ 117,\ 437, \tag{6}$$

of the form $D = n^2 - 4$, and Chowla [11] conjectured that there are six such discriminants of the form $4n^2 + 1$:

$$D = 5,\ 17,\ 37,\ 101,\ 197,\ 677. \tag{7}$$

To yield nontrivial lower bounds on $h(D)$ in families where the regulator grows like $\log(D)$, Goldfeld's inequality (3) would require a Hasse–Weil L-function with a zero of order $\varrho \geq 4$, whose existence follows from the Birch and Swinnerton-Dyer conjecture but has yet to be established unconditionally. In spite of this difficulty, Biró was able to prove Yokoi's conjecture [7] and Chowla's conjecture [6] by a relatively elementary approach exploiting explicit formulas for special values of zeta functions attached to ideal classes in real quadratic fields (see [8]) and Byeon, Lee and Kim [9] managed to adapt Biró's method to settle the $n^2 - 4$ case. Further recent progress based on Goldfeld's method has been achieved in [35].

In conclusion, the Goldfeld–Gross–Zagier approach can, with some further effort, be applied to real quadratic fields. Adapting the Heegner–Stark approach presents a different kind of difficulty, since it would require an extension of the theory of

complex multiplication to the setting of real quadratic fields. A largely conjectural theory of "real multiplication" was proposed in [14] and developed further in [15] and [16], so that the main arithmetic objects arising in the theory of complex multiplication — singular moduli, elliptic units, and Heegner points — now admit well-documented analogues in this framework.

Our main goal is to explain how the *Stark–Heegner points* of the title provide the basis for a natural — albeit *conditional* — solution, modelled on the Heegner–Stark approach, to various class number one problems for real quadratic fields like the conjectures of Yokoi, Mollin and Chowla evoked above.

Section 3 briefly recapitulates the theory of Stark–Heegner points, whose key predictions are summarised in Conjectures 7 and 26. The main theorem of this paper is:

Main Theorem. *Assume Conjecture 7 of Section 3. Then the conjectures of Yokoi, Mollin and Chowla are true.*

To sketch the proof of this theorem, the "rigid analytic elliptic cocycle" attached to an elliptic curve E of prime conductor p yields an explicit rigid analytic function $\Phi_E(\tau)$ on the Drinfeld p-adic upper half-plane,

$$\mathfrak{H}_p := \mathbb{P}_1(\mathbb{C}_p) - \mathbb{P}_1(\mathbb{Q}_p),$$

which enjoys a number of remarkable properties. For instance, letting

$$D := n^2 + 4, \quad \varepsilon_D := \tfrac{1}{2}(n + \sqrt{n^2+4}) \qquad \text{with } n \geq 1,$$

the image of $\Phi_E(\varepsilon_D)$ in $E(\mathbb{C}_p)$ under the Tate uniformisation is expected to be a global point on E — a so-called *Stark–Heegner point* — defined over the ring class field H_D. In particular, this point should belong to $E(K_D)$ if $h(D) = 1$. The conjectural Gross–Zagier formula for Stark–Heegner points spelled out in Conjecture 7(2) of Section 3 further predicts the triviality of this quadratic point if E has analytic rank ≥ 2 over $\mathbb{Q}$; it follows in this case that, for $D = n^2 + 4$,

$$\Phi_E(\varepsilon_D) = 1 \quad \text{whenever } h(D) = 1.$$

When n is larger than $p+2$ and p does not divide D, it is shown in Section 1 that the quadratic elements ε_D must lie in $\mathfrak{H}_p$ and even in the standard affinoid subset $\mathfrak{H}_p^\circ \subset \mathfrak{H}_p$ consisting of the complement in $\mathbb{P}_1(\mathbb{C}_p)$ of the $(p+1)$ distinct $\mathbb{F}_p$-rational mod p residue discs. To deduce Yokoi's conjecture from the conjectured properties of Φ_E, it therefore essentially suffices to verify that all the zeroes of $\Phi_E(\tau) - 1$ in $\mathfrak{H}_p^\circ$ that are quadratic over $\mathbb{Q}_p$ and of norm -1 are accounted for by the class number one discriminants listed in (5).

Thanks to Hensel's lemma, understanding the zeroes of $\Phi_E(\tau) - 1$ in $\mathfrak{H}_p^\circ$ can largely be reduced to the study of the mod p reduction of $\Phi_E(z)$, denoted by $R_E(x)$.

It is a rational function on $\mathbb{P}_1$ over $\mathbb{F}_p$ with all its zeroes and poles in $\mathbb{P}_1(\mathbb{F}_p)$. A formula for $R_E(x)$ is available in terms of the *Manin symbols* for E, and the factorisation of $R_E(x) - 1$ over $\mathbb{F}_p$ is readily carried out by computer.

For example, the smallest elliptic curve of rank two and prime conductor arises when $p = 389$. For this elliptic curve, denoted by $389A1$ in the tables of Cremona, the degree of $R_E(x)$ is 144. Assuming Conjecture 7 on Stark–Heegner points, a study of the zeroes of $R_E(x) - 1$ implies that any class number one discriminant of the form $n^2 + 4$ not appearing in (5) must be divisible by 389. Several other elliptic curves of rank two also yield the analogous result, and the full determination follows from genus theory, as will be explained further in Section 6.

The same strategy applies to the discriminants D of the form $n^2 - 4$, leading to the conclusion that (6) is a complete list of the class number one discriminants of that form. Modifications of Φ_E can also be constructed to tackle Chowla's conjecture, or more general class number one problems for real quadratic fields of *Richaud–Degert type*, as explained in Section 7.

The situation is somewhat reminiscent of Skolem's p-adic method and its more elaborate version by Chabauty and Coleman, which produces a nonconstant p-adic analytic function on a curve that vanishes at all of its integral points. One gets a full determination of the set of integral points by examining the zeroes of this function, provided it has no extraneous ones. The function $\Phi_E(z) - 1$ fills an analogous role for the class number one discriminants of the form $n^2 \pm 4$. The Heegner–Stark approach to Yokoi's conjecture is thus imbued with a diophantine flavour, even if the diophantine aspects of the theory of Stark–Heegner points remain rather mysterious. See [10, Chapter 4, Section 6 and Chapter 10, Section 10] for a nice overview of Skolem's p-adic method, and [2] and [3] for a discussion of an anabelian refinement of the Chabauty–Coleman method, with applications to certain modular curves of level 13 and 17 with direct relevance to the Gauss class number problem.

We close the introduction with three remarks:

(1) The names of Heegner and Stark appeared in [14] because of a sentiment that "Stark–Heegner points are to Heegner points what (Gross–)Stark units are to elliptic or circular units". That the Heegner–Stark method can be adapted to real quadratic fields thanks to the eponymous points is a happy but entirely fortuitous circumstance which was not anticipated when the terminology was coined.

(2) It is amusing that a conjectural Gross–Zagier formula for Stark–Heegner points applied to certain elliptic curves of rank > 1 features prominently in a strategy which otherwise has very little in common with the approach of Goldfeld–Gross–Zagier.

(3) Readers inclined to take the jaundiced view may question the value of a conditional proof, relying on a highly conjectural theory, of theorems which are in many cases already known. Aside from its aesthetic appeal, the authors hope that the

approach they describe provides convincing if somewhat oblique evidence for the theory of Stark–Heegner points by subjecting it to an exacting "stress test", much as physicists validate their theories by showing that they accurately predict certain experimental outcomes.

1. Splitting of small primes in real quadratic fields

In this section, we prove that, if $D = n^2 \pm 4$ is a fundamental discriminant of class number one, then the small primes $p < n+2$ are either inert or ramified in $K_D/\mathbb{Q}$. This implies that the RM points of discriminant $D = n^2 \pm 4$ belong to $\mathfrak{H}_p$ so long as $n > p+2$, a crucial property which allows the classification of such D to be tackled with the theory of real multiplication and Stark–Heegner points.

The following proposition seems to be folklore (see for instance [27, Lemma 1] and [7, Fact B]) but we include a proof for the sake of completeness. It is the real quadratic analogue of the classical fact that every prime strictly smaller than $\frac{1}{4}|D|$ is inert in K_D when D is a negative discriminant of class number one.

Proposition 1. *Let $D > 0$ be a discriminant of class number one and let v be the conductor of $\mathbb{Z}[\varepsilon_D]$ relative to $\mathcal{O}_D$. Then every prime $p < \frac{1}{v}(\sqrt{D}-2)$ is inert in $\mathcal{O}_D$ or divides its conductor.*

Remark 2. This bound is sharp: if $D = n^2 - 4$ has class number one and $p = n-2$ is prime, p ramifies, so the -2 in the numerator is necessary. Nonetheless, it is not hard to see from our proof that this is the only case in which we cannot replace the bound by $\frac{1}{v}(\sqrt{D}-1)$.

Corollary 3. *Let $D > 0$ be a discriminant of class number one and of the form $n^2 \pm 4$. Then any prime $p < n-2$ which doesn't divide the conductor of D is inert in K_D.*

Proof. In this case, $\frac{1}{2}(n+\sqrt{D})$ is a power of the fundamental unit ε_D. Since $\mathbb{Z}\left[\frac{1}{2}(n+\sqrt{D})\right] = \mathcal{O}_D$ already has conductor 1, the same holds for $\mathbb{Z}[\varepsilon_D]$. □

To prove Proposition 1, we use the following lemma.

Lemma 4. *Let $D > 0$ be a positive discriminant and let v be the conductor of $\mathbb{Z}[\varepsilon_D]$ relative to $\mathcal{O}_D$. If $\alpha \in \mathcal{O}_D$ is such that*

$$|\mathrm{Norm}_{K_D/\mathbb{Q}}(\alpha)| < \frac{\sqrt{D}-2}{v},$$

then α is associated to a rational integer.

Proof. Set $\varepsilon = \varepsilon_D = u + v\sqrt{D}/2$, where $u, v > 0$. The statement is vacuous if $u \leq \frac{3}{2}$ (since then $\sqrt{D} - 2 < 2$) so we may assume $u \geq 2$. As $4u^2 - Dv^2 = \pm 4$, we have

$$D = \frac{4u^2 \mp 4}{v^2} \leq \left(\frac{2u+1}{v}\right)^2.$$

In particular, since $\sqrt{D} \le (2u+1)/v$, it suffices to prove the claim for α of norm at most $(2u-2)/v^2$. In the same way, we obtain $D \ge ((2u-1)/v)^2$ and so

$$|\varepsilon^{-1}| = \frac{1}{u + \frac{1}{2}v\sqrt{D}} \le \frac{1}{2u-1}.$$

Set $v\alpha = a\varepsilon^{-1} + b$ for some rational integers a, b. After possibly multiplying α by a power of epsilon, we may assume that $\varepsilon^{-1} \le |v\alpha| \le 1$. If $a = 0$ then α is already rational so suppose $a > 0$. The conjugate $\overline{\alpha}$ of α satisfies

$$v|\overline{\alpha}| = |a\varepsilon \pm b| = |a(\varepsilon \mp \varepsilon^{-1}) \pm v\alpha| \ge a(\varepsilon \mp \varepsilon^{-1}) - 1.$$

It follows that

$$v^2|\alpha\overline{\alpha}| \ge \varepsilon^{-1}(a(\varepsilon \mp \varepsilon^{-1}) - 1) \ge a(1 - \varepsilon^{-2}) - \varepsilon^{-1}.$$

On the other hand, if $a \ge 2u-1$, we have

$$a(1-\varepsilon^{-2}) - \varepsilon^{-1} > (2u-1)\left(1 - \frac{1}{(2u-1)^2}\right) - \frac{1}{2u-1} \ge 2u-2.$$

We conclude that $a < 2u-1$, from which we deduce $0 < a\varepsilon^{-1} < 1$. As $|v\alpha| \le 1$, we must have $b = 0$ or $b = -1$. If $b = 0$ we are done, and if $b = -1$ we find

$$2u - 2 \ge v^2|\alpha\overline{\alpha}| = a(2u-a) \mp 1,$$

which impossible as $0 < a \le 2u-2$. □

Proof of Proposition 1. Suppose $p < (\sqrt{D}-2)/v$ is a prime which is not inert and doesn't divide the conductor of $\mathcal{O}_D$. Then, since D has class number one, $\pm p$ is represented by the principal form, i.e., we can write $\pm p$ as the norm of some element $\alpha \in \mathcal{O}_D$. Lemma 4 then implies that p is a square, a contradiction. □

2. Modular parametrisations and elliptic cocycles

We begin with a presentation of classical modular parametrisations of elliptic curves designed to motivate their p-adic counterparts: the *rigid analytic elliptic cocycles* that are the basis for the theory of Stark–Heegner points.

Let E be an elliptic curve of conductor N, and let

$$a_\ell(E) = \ell + 1 - \#E(\mathbb{F}_\ell) \quad \text{for all primes } \ell \nmid N.$$

The first cohomology $H^1(\Gamma_0(N), \mathbb{Z})$ of the Hecke congruence group $\Gamma_0(N)$ is endowed with an action of Hecke operators, and the modularity theorem of Wiles and Taylor–Wiles asserts that there are two classes φ_E^+ and $\varphi_E^- \in H^1(\Gamma_0(N), \mathbb{Z})$ satisfying

$$\varphi_E^\pm \begin{pmatrix} a & -b \\ -c & d \end{pmatrix} = \pm\varphi_E^\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad T_\ell(\varphi_E^\pm) = a_\ell(E)\cdot\varphi_E^\pm \quad \text{for all } \ell \nmid N.$$

Wiles' proof produces suitable eigenclasses in the étale cohomology of the modular curve $X_0(N)$, from which the classes $\varphi_E^{\pm}$ are deduced via comparison theorems between étale and singular cohomology.

The group $\Gamma_0(N)$ acts discretely on the Poincaré upper half-plane $\mathfrak{H}$ by Möbius transformations, and hence on the additive group $\mathcal{O}_{\mathfrak{H}}$ of holomorphic functions on $\mathfrak{H}$. Faltings' proof of the isogeny conjecture for abelian varieties implies the following proposition:

Proposition 5. *There are two complex numbers $\Omega_E^+ \in \mathbb{R}$ and $\Omega_E^- \in i\mathbb{R}$ satisfying the following conditions*:

(1) *The lattice $\Lambda_E := \mathbb{Z}\Omega_E^+ + \mathbb{Z}\Omega_E^-$ is commensurable with the Néron lattice of E.*

(2) *The class*

$$\Omega_E^+ \cdot \varphi_E^+ + \Omega_E^- \cdot \varphi_E^- \in H^1(\Gamma_0(N), \mathbb{C}) \tag{8}$$

is in the kernel of the natural map

$$H^1(\Gamma_0(N), \mathbb{C}) \to H^1(\Gamma_0(N), \mathcal{O}_{\mathfrak{H}}).$$

In particular, there is a 0-cochain $\mathcal{J}_E \in C^0(\Gamma_0(N), \mathcal{O}_{\mathfrak{H}})$ satisfying

$$\mathcal{J}_E(\gamma^{-1}z) - \mathcal{J}_E(z) = \Omega_E^+ \cdot \varphi_E^+(\gamma) + \Omega_E^- \cdot \varphi_E^-(\gamma) \quad \text{for all } \gamma \in \Gamma_0(N). \tag{9}$$

The resulting function

$$\mathcal{J}_E : \Gamma_0(N)\backslash\mathfrak{H} \to \mathbb{C}/\Lambda_E \simeq E(\mathbb{C}) \tag{10}$$

is called the *modular parametrisation* attached to E. An important application of $\mathcal{J}_E$ is the construction of a plentiful and arithmetically interesting supply of algebraic points on E which are the basis for the best known results towards the Birch and Swinnerton-Dyer conjecture: the *Heegner points* arising from the image of (imaginary) quadratic arguments in $\mathfrak{H}$. Namely, letting $\mathfrak{H}^{\mathrm{CM}}$ be the set of points of $\mathfrak{H}$ satisfying a quadratic equation over $\mathbb{Q}$, the holomorphic function $\mathcal{J}_E$ on $\mathfrak{H}$ induces a map

$$\mathcal{J}_E : \mathfrak{H}^{\mathrm{CM}} \to E(\mathbb{C}), \tag{11}$$

whose image lies in the Mordell–Weil groups of E over ring class fields of quadratic imaginary fields.

We now turn to elliptic cocycles which are a p-adic analogue of the modular parametrisation $\mathcal{J}_E$ of (11) suitable for a theory of real multiplication.

Suppose p is a prime at which E has *multiplicative reduction*. The periods $\Omega_E^{\pm}$ (or rather, the complex exponential of $2\pi i \cdot \Omega_E^-/\Omega_E^+$) then admit a p-adic analogue, the Tate period $q \in \mathbb{Q}_p^{\times}$ attached to E, for which

$$E(\mathbb{C}_p) = \mathbb{C}_p^{\times}/q^{\mathbb{Z}}. \tag{12}$$

The prime p necessarily divides the conductor N of E. For simplicity, and because this is the only case that will arise in the application to the class number one problem, assume from now on that $N = p$.

The class in (8) admits two natural p-adic multiplicative counterparts arising from the map on cohomology induced by the homomorphism from $\mathbb{Z}$ to $\mathbb{Q}_p^\times$ sending k to q^k, namely,

$$q^{\varphi_E^+},\ q^{\varphi_E^-} \in H^1(\Gamma_0(p), \mathbb{Q}_p^\times).$$

To transpose the discussion of the previous section to a p-adic setting, it is natural to replace $\mathfrak{H}$ by the Drinfeld p-adic upper half-plane

$$\mathfrak{H}_p := \mathbb{P}_1(\mathbb{C}_p) - \mathbb{P}_1(\mathbb{Q}_p)$$

equipped with its structure of a rigid analytic space. Let $\mathcal{O}_{\mathfrak{H}_p}$ denote the ring of rigid analytic functions on $\mathfrak{H}_p$. The group $\Gamma_0(p)$ acts on $\mathfrak{H}_p$ by Möbius transformations, and hence on $\mathcal{O}_{\mathfrak{H}_p}^\times$, but the class q^{φ_E} is not trivialised under the natural inclusion $\mathbb{Q}_p^\times \to \mathcal{O}_{\mathfrak{H}_p}^\times$. This is because the analogue of the cochain J_E of (9) would have to be invariant under integer translations, and $\mathbb{Z}$ is not discrete p-adically, but dense in $\mathbb{Z}_p$.

It turns out to be fruitful to replace $\Gamma_0(p)$ by the larger *Ihara group* $\Gamma := \mathrm{SL}_2(\mathbb{Z}[1/p])$, which is an amalgamated product

$$\Gamma = \mathrm{SL}_2(\mathbb{Z}) *_{\Gamma_0(p)} \mathrm{SL}_2(\mathbb{Z}).$$

The Mayer–Vietoris sequence in group cohomology supplies an injective map

$$H^1(\Gamma_0(p), \mathbb{Z}) \to H^2(\Gamma, \mathbb{Z})$$

with finite cokernel. Let $\alpha_E^+, \alpha_E^- \in H^2(\Gamma, \mathbb{Z})$ be the images of φ_E^+ and φ_E^- respectively, under this map.

The following conjecture is a p-adic counterpart of Proposition 5 in which the degree of cohomology is shifted by one:

Conjecture 6 [14, Conjecture 5]. *The classes*

$$q^{\alpha_E^+},\ q^{\alpha_E^-} \in H^2(\Gamma, \mathbb{Q}_p^\times)$$

lie in the kernel of the natural map

$$H^2(\Gamma, \mathbb{Q}_p^\times) \to H^2(\Gamma, \mathcal{O}_{\mathfrak{H}_p}^\times).$$

Conjecture 6 is obtained by formally exponentiating the formula in [14, Theorem 4], which is itself deduced as a formal consequence of the exceptional zero conjecture of Mazur, Tate and Teitelbaum [24] proved by Greenberg and Stevens [19]. The tame refinement of the Greenberg–Stevens theorem proved in [31] leads to a statement that is almost as strong as Conjecture 6 up to a supplementary torsion ambiguity, at least for elliptic curves that are unique in their rational isogeny class.

Conjecture 6 implies that there are one-cochains J_E^+ and $J_E^- \in C^1(\Gamma, \mathcal{O}_{\mathfrak{H}_p}^\times)$ satisfying

$$J_E^\pm(\gamma_2)(\gamma_1^{-1}z) \div J_E^\pm(\gamma_1\gamma_2)(z) \times J_E^\pm(\gamma_1)(z) = q^{\alpha_E^\pm(\gamma_1,\gamma_2)} \quad \text{for all } \gamma_1, \gamma_2 \in \Gamma.$$

The natural images of J_E^+ and J_E^- in $H^1(\Gamma, \mathcal{O}_{\mathfrak{H}_p}^\times/q^{\mathbb{Z}})$ are called the (even and odd, respectively) *rigid analytic elliptic cocycles* attached to E. They play much the same role as the modular parametrisation of E in (10) in the setting of real multiplication theory, as will be explained in the next section.

The construction in [14] shows that the cocycles $J_E^\pm$ can be represented by parabolic cocycles which are trivial on the standard parabolic subgroup, and hence can also be described as a Γ-invariant modular symbol with values in $\mathcal{O}_{\mathfrak{H}_p}^\times/q^{\mathbb{Z}}$. This point of view, which is convenient for explicit calculations, will be systematically adopted from now on, namely, the symbols $J_E^\pm$ will be used interchangeably to describe parabolic one-cocycles on Γ and their associated modular symbol. Hence the cocycles J_E^+ and J_E^- are now to be envisaged as functions

$$J_E^+, J_E^- : \mathbb{P}_1(\mathbb{Q}) \times \mathbb{P}_1(\mathbb{Q}) \to \mathcal{O}_{\mathfrak{H}_p}^\times/q^{\mathbb{Z}}$$

satisfying the usual additivity properties of modular symbols,

$$J_E^\pm\{r,s\} = J_E^\pm\{s,r\}^{-1}, \quad J_E^\pm\{r,s\} \times J_E^\pm\{s,t\} = J_E^\pm\{r,t\} \qquad \text{for all } r,s,t \in \mathbb{P}_1(\mathbb{Q}),$$

as well as an invariance property under Γ,

$$J_E^\pm\{\gamma r, \gamma s\}(\gamma\tau) = J_E^\pm\{r,s\}(\tau) \quad \text{for all } \gamma \in \Gamma.$$

The cohomology class c can be recovered from its associated Γ-invariant modular symbol m by choosing a basepoint $t \in \mathbb{P}_1(\mathbb{Q})$ and setting

$$c(\gamma) := m\{t, \gamma t\}.$$

3. Stark–Heegner points

An element $\tau \in \mathfrak{H}_p$ is called an RM point if it satisfies a quadratic equation with integer coefficients and positive discriminant. The field $K_\tau = \mathbb{Q}(\tau)$ is then a real quadratic field in which p is nonsplit, and the $\mathbb{Z}[1/p]$-order

$$\mathcal{O}_\tau^{(p)} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}[1/p]) \text{ such that } c\tau^2 + (d-a)\tau - b = 0 \right\}$$

is isomorphic to a $\mathbb{Z}[1/p]$-order in K_τ, embedded via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto c\tau + d.$$

The discriminant of $\mathcal{O}_\tau^{(p)}$ (a positive integer which is not divisible by p^2 if p is odd, by definition) is also called the discriminant of τ.

The stabiliser of τ in $\mathrm{GL}_2(\mathbb{Z}[1/p])$, denoted by Γ_τ, is isomorphic to the group $\mathcal{O}_\tau^{(p)\times}$ of units in $\mathcal{O}_\tau^{(p)}$, and hence is of rank one. A generator γ_τ for Γ_τ, which we call the *fundamental automorph* of τ, can be normalised by choosing the fundamental unit $\varepsilon_\tau > 1$ of $\mathcal{O}_\tau^{(p)}$, embedding it into $\mathbb{C}_p$, and requiring that γ_τ act on the column vector $(\tau, 1)$ as multiplication by ε_τ. The *value* of J_E^+ at $\tau \in \mathfrak{H}_p^{\mathrm{RM}}$ is then defined by setting

$$J_E^+[\tau] := J_E^+(\gamma_\tau)(\tau) = J_E^+\{0, \gamma_\tau 0\}(\tau) \in \mathbb{C}_p^\times/q^{\mathbb{Z}} = E(\mathbb{C}_p).$$

(To evaluate the odd cocycle J_E^-, it is necessary to replace γ_τ by a generator of the stabiliser of τ in $\Gamma \subset \mathrm{GL}_2(\mathbb{Z}[1/p])$ modulo torsion, i.e., to replace γ_τ by its square when the fundamental unit of $\mathcal{O}_\tau^{(p)}$ has norm -1.)

The value of $J_E^\pm$ at an RM point τ only depends on the cohomology class of $J_E^\pm$: if $\varphi(\gamma) = f^{-1} \cdot (\gamma f)$ is a one-coboundary, then

$$\varphi[\tau] = f(\gamma_\tau^{-1}\tau) f(\tau)^{-1} = 1.$$

Moreover, the assignment $\tau \mapsto J_E^\pm[\tau]$ is Γ-invariant: if $\gamma \in \Gamma$, the fundamental automorph of $\gamma\tau$ is $\gamma\gamma_\tau\gamma^{-1}$ and we have

$$J_E^\pm[\gamma\tau] = J_E^\pm(\gamma\gamma_\tau\gamma^{-1})(\gamma\tau) = J_E^\pm(\gamma)(\gamma\tau) \times J_E^\pm(\gamma_\tau)(\tau) \times J_E^\pm(\gamma^{-1})(\tau) = J_E^\pm[\tau].$$

The cocycles J_E^+ and J_E^- thus yield two maps

$$J_E^+, J_E^- : \Gamma\backslash\mathfrak{H}_p^{\mathrm{RM}} \to E(\mathbb{C}_p) \tag{13}$$

directly analogous to (11), where $\mathfrak{H}_p^{\mathrm{RM}}$ denotes the set of RM points in $\mathfrak{H}_p$. The main conjecture of [14] (see [14, Conjectures 5.6, 5.15]) predicts that the image of J_E^+ (resp. J_E^-) lies in the union of the Mordell–Weil groups of E over all ring class fields in the wide (resp. narrow) sense of real quadratic fields, suggesting the construction of a plentiful and arithmetically interesting supply of algebraic points on E, the so-called *Stark–Heegner points*:

Conjecture 7. (1) *If $\tau \in \mathfrak{H}_p^{\mathrm{RM}}$ is an RM point with (not necessarily maximal) associated order $\mathcal{O}_\tau = \mathcal{O}_D$, then the image of $J_E^+[\tau]$ (resp. $J_E^-[\tau]$) under (12) is a global point of E defined over the ring class field H_D (resp. the **narrow ring class field**) attached to D.*

(2) (*Gross–Zagier formula*) *For D a fundamental discriminant,*

$$\mathrm{ht}_E(\mathrm{Trace}_{K_D}^{H_D}(J_E^+[\tau])) \sim L'(E/K, 1), \tag{14}$$

where ht_E is the Néron–Tate canonical height on E over K_D, and $\sim$ denotes an equality up to an explicit nonzero fudge factor.

Remark 8. Conjecture 7 can be supplemented with a conjectural Shimura reciprocity law [14, Conjecture 5.9], which allows the trace in (2) to be expressed as

a sum over the class group rather than over the Galois group of H_D/K_D. This makes (2) somewhat more independent of (1).

Remark 9. If D is not a fundamental discriminant, and ℓ is an odd prime whose square divides it exactly, then the Stark–Heegner points of discriminants D and $D_0 := D/\ell^2$ are related by the same norm-compatibility relations as classical Heegner points:

$$\mathrm{Trace}_{H_{D_0}}^{H_D}(J_E^+[\tau_D]) = \begin{cases} (a_\ell(E) - \mathrm{frob}_\lambda - \mathrm{frob}_{\lambda'})J_E^+[\tau_{D_0}] & \text{if } \ell = \lambda\lambda' \text{ in } K_D/\mathbb{Q}, \\ a_\ell(E)J_E^+[\tau_{D_0}] & \text{if } \ell \text{ is inert in } K_D/\mathbb{Q}, \end{cases} \tag{15}$$

for a suitable τ_{D_0} of discriminant D_0, where the traces and frobenius elements are to be understood as elements of (the group ring of) the class group via the reciprocity law of global class field theory for K_D. The Gross–Zagier formula (14) can be extended to nonfundamental discriminants of the form $D = D_0c^2$ with D_0 fundamental and $c = \ell_1 \cdots \ell_m \cdot q_1 \cdots q_n$ an odd squarefree product of rational primes in which the ℓ_i are split and the q_j are inert in $K_D/\mathbb{Q}$, by the formula

$$\mathrm{ht}_E(\mathrm{Trace}_{K_D}^{H_D}(J_E^+[\tau])) \sim \prod_{i=1}^{m}(a_{\ell_i}(E) - 2)^2 \prod_{j=1}^{n} a_{q_j}(E)^2 \cdot L'(E/K, 1). \tag{16}$$

Remark 10. While Conjecture 7(1) seems inaccessible short of an essentially new idea, Conjecture 7(2) might be amenable to the methods of [5] and [25], where the p-adic logarithms of the traces of Stark–Heegner points to certain *genus fields* of real quadratic fields are shown to agree with the p-adic logarithms of global points, by a comparison with Heegner points arising from suitable Shimura curve parametrisations. It does not seem out of the question that a tame refinement of this approach and its extension in the spirit of de Shalit's proof [31] of a tame refinement of the theorem of Greenberg–Stevens could eventually lead to a proof of, or at least partial theoretical evidence for, Conjecture 7(2).

The special case of Conjecture 7 that is germane to the class number one problem for real quadratic fields involves only the even cocycle J_E^+, which shall henceforth be denoted by J_E to lighten the notation.

A simple but crucial observation is that if

$$L(E/\mathbb{Q}, 1) = L'(E/\mathbb{Q}, 1) = 0,$$

the L-series derivative that appears in Conjecture 7(2) always vanishes. The non-degeneracy of the Néron–Tate height then implies that the trace to K_τ of the Stark–Heegner point $J_E[\tau]$ is torsion. This leads to a nontrivial property of the class number one real quadratic orders in which p is inert:

Corollary 11. *Assume Conjecture 7. If E is an elliptic curve of prime conductor p and analytic rank ≥ 2, and D is a discriminant of class number one for which $(D/p) = -1$, then $J_E\left[\frac{1}{2}(D+\sqrt{D})\right]$ maps to a torsion point in $E(K_D)$ under (12). In particular, $J_E\left[\frac{1}{2}(D+\sqrt{D})\right] = 1$ if E has trivial torsion over quadratic fields.*

Remark 12. If E is any elliptic curve over $\mathbb{Q}$, then $E(K_D)_{\mathrm{tor}} = E(\mathbb{Q})_{\mathrm{tor}}$ for all but finitely discriminants D. Moreover, the list of exceptional D's can be found in the LMFDB database entry for E (under "growth of torsion in number fields"). It turns out that all elliptic curves over $\mathbb{Q}$ of analytic rank ≥ 2 and prime conductor ≤ 10000 have trivial torsion over quadratic fields.

Remark 13. The assumption on the analytic rank is implied by a similar assumption on the algebraic rank, thanks to the deep results of Gross–Zagier and Kolyvagin. The converse is still open and very little is known about it without assuming the Birch and Swinnerton-Dyer conjecture or at least the Shafarevich–Tate conjecture. This is why we have phrased Corollary 11 in terms of the weaker assumption on the analytic rank.

Although Corollary 11 gives a nontrivial property satisfied by *all* real quadratic discriminants of class number one, it is unclear whether it brings us any closer to understanding the class number one problem for real quadratic fields. Since J_E is a cocycle and not a function, its fibers are clearly not finite: indeed if they were it would contradict the widely believed infinitude of D for which $h(D) = 1$.

4. Rigid analytic period functions

The (even) *rigid analytic period function* attached to E is simply the rigid analytic function on $\mathfrak{H}_p$ defined by

$$\Phi_E(z) := J_E\{0, \infty\}.$$

There is no loss of information in passing from J_E to its associated rigid analytic period function. Indeed, the Euclidean algorithm for the gcd implies that any path from one cusp to another can be expressed as a finite sum of *unimodular paths*, of the form $\{a/b, c/d\}$ with $ad - bc = \pm 1$, and these unimodular paths are all equivalent under Γ (under $\mathrm{GL}_2(\mathbb{Z})$, in fact) to $\{0, \infty\}$.

The rigid analytic period function Φ_E is far from being invariant under Γ, but it is invariant under $z \mapsto -z$ (because J_E is even) and under the map $z \mapsto p^2 z$. It also satisfies the two- and three-term relations

$$\Phi_E\left(\frac{1}{z}\right) = \Phi_E(z)^{-1} \quad \text{and} \quad \frac{\Phi_E(z+1)}{\Phi_E(z)} = \Phi_E\left(\frac{z+1}{z}\right), \tag{17}$$

as well as some further more complicated functional equations whose precise nature depends on the prime p.

The value of the cocycle J_E at $\tau \in \mathfrak{H}_p^{\mathrm{RM}}$ can be expressed as a product of values of Φ_E at a collection of $\mathrm{GL}_2(\mathbb{Z})$-translates of τ arising from its continued fraction expansion (viewed as a real number)

$$\tau = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} \quad \text{with } a_i \in \mathbb{Z}^{\geq 1}.$$

The number τ is real quadratic if and only if $(a_0, a_1, \dots)$ is *eventually periodic*, and it is said to be *reduced* if $(a_0, a_1, \dots)$ is *periodic*. This is equivalent to the condition

$$\tau > 1, \quad -1 < \tau' < 0,$$

where τ' is the algebraic conjugate of τ. Assume now that τ is reduced and that its continued fraction expansion has minimal period length m. Then, denoting by $[x]$ the integer part of a positive real number x, we can write

$$\begin{aligned}
\tau_0 &= \tau, & a_0 &= [\tau_0], \\
\tau_1 &= (\tau_0 - a_0)^{-1}, & a_1 &= [\tau_1], \\
\tau_2 &= (\tau_1 - a_1)^{-1}, & a_2 &= [\tau_2], \\
&\vdots & &\vdots \\
\tau_{m-1} &= (\tau_{m-2} - a_{m-2})^{-1}, & a_{m-1} &= [\tau_{m-1}], \\
\tau_m &= (\tau_{m-1} - a_{m-1})^{-1}, & \tau_m &= \tau_0.
\end{aligned}$$

The sequence $(\tau_0, \tau_1, \dots, \tau_{m-1})$ is called the *reduced cycle* attached to $\tau_0 = \tau$. The τ_i represent the roots of binary quadratic forms in a cycle of reduced forms of discriminant D.

Lemma 14. *The value of the even elliptic cocycle J_E at a reduced $\tau \in \mathfrak{H}_p^{\mathrm{RM}}$ is given by*

$$J_E[\tau] := \Phi_E(\tau_0) \cdot \Phi_E(\tau_1) \cdot \Phi_E(\tau_2) \cdots \Phi_E(\tau_{m-2}) \cdot \Phi_E(\tau_{m-1}).$$

Proof. Let $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$. For each $i < m$, set $\gamma_i = T^{a_i} S$ so that $\tau_{i+1} = \gamma_i^{-1} \tau_i$. Set $\gamma = \gamma_0 \cdots \gamma_{m-1}$. The periodicity of the continued fraction of τ implies that $\gamma \tau = \tau$. Conversely, since τ is reduced, the fundamental automorph γ_τ of τ has nonnegative coefficients and its top-left entry is maximal so the Euclidean algorithm shows it can be written as $T^{b_0} S T^{b_1} S \cdots T^{b_{m-1}} S$ for some positive integers $b_0, \dots, b_{m-1} \geq 1$. The equality $\gamma_\tau \tau = \tau$ then translates to $[\overline{b_0, \dots, b_{m-1}}]$ being the continued fraction of τ. It follows from the uniqueness of the continued fraction

that $\gamma = \gamma_\tau$ is the fundamental automorph of τ. Accordingly,

$$J_E[\tau] = J_E\{0, \gamma_\tau 0\}(\tau) = \prod_{i=0}^{m-1} J_E\{\gamma_0 \cdots \gamma_{i-1} 0, \gamma_0 \cdots \gamma_i 0\}(\tau)$$
$$= \prod_{i=0}^{m-1} J_E\{0, \gamma_i 0\}(\gamma_{i-1}^{-1} \cdots \gamma_0^{-1} \tau) = \prod_{i=0}^{m-1} \Phi_E(\tau_i). \quad \square$$

It transpires from Lemma 14 that $J_E[\tau]$ is a product of values of Φ_E, the number of factors in the product depending on the length of the period in the continued fraction expansion of τ.

Most importantly, when D is of the form $n^2 + 4$, we can express $J_E[\tau]$ as a *single value* of the rigid analytic period function Φ_E at

$$\varepsilon_D := \frac{n + \sqrt{n^2+4}}{2} = n + \cfrac{1}{n + \cfrac{1}{n + \cdots}}. \tag{18}$$

The same is true with discriminants of the form $D = n^2 - 4$, where

$$\varepsilon_D = \tfrac{1}{2}(n + \sqrt{n^2 - 4})$$

except when $D = 5$ and $n = 3$, where this unit of norm 1 is the square of the golden ratio ε_D.

Proposition 15. *For all D of the form $n^2 \pm 4$,*

$$J_E\big[\tfrac{1}{2}(D + \sqrt{D})\big] = \Phi_E(\varepsilon_D).$$

If $D = 5$, then furthermore

$$J_E\big[\tfrac{1}{2}(1 + \sqrt{5})\big] = \Phi_E(\varepsilon_5) \quad \textit{and} \quad J_E\big[\tfrac{1}{2}(1 + \sqrt{5})\big]^2 = \Phi_E(\varepsilon_5^2).$$

Proof. For $D = n^2 + 4$, this follows from Lemma 14 combined with (18). In general, one can directly see that the fundamental automorph attached to the unit ε_D of norm $s = \pm 1$ is

$$\gamma_D = \begin{pmatrix} n & -s \\ 1 & 0 \end{pmatrix},$$

so that

$$J_E\big[\tfrac{1}{2}(D + \sqrt{D})\big] = J_E[\varepsilon_D] = J_E\{0, \gamma_D 0\}(\varepsilon_D) = J_E\{0, \infty\}(\varepsilon_D) = \Phi_E(\varepsilon_D).$$

The discriminant $D = 5$ is exceptional because it is the only discriminant which can be written as both $n^2 + 4$ and $n^2 - 4$. In the latter case, $\frac{1}{2}(3 + \sqrt{3^2 - 4}) = \varepsilon_5^2$ is actually the square of the fundamental unit $\varepsilon_5 = \frac{1}{2}(1 + \sqrt{5})$. For the same reason $\left(\begin{smallmatrix} 3 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ is the square of the automorph γ_5, so the above computation yields

$$\Phi_E(\varepsilon_5^2) = J_E\big[\tfrac{1}{2}(1 + \sqrt{5})\big]^2. \quad \square$$

Proposition 15 leads to the following concrete consequence of Corollary 11:

Corollary 16. *Assume Conjecture 7. Let E be an elliptic curve of prime conductor p and analytic rank ≥ 2 over $\mathbb{Q}$ having no quadratic torsion. If $D = n^2 \pm 4$ is the discriminant of a quadratic field of class number one in which p is inert, then $\Phi_E(\varepsilon_D) = 1$. If p is inert in K_5, then $\Phi_E(\varepsilon_5^2) = 1$ as well.*

For the negative discriminants $D = -4$ and $D = -3$ that occur in (6), a substantial part of the natural analogue of Corollary 16 can be proven independently of Conjecture 7. More precisely, if K is any imaginary quadratic field in which p is inert and $\tau \in \mathfrak{H}_p \cap K$, we can define $J_E[\tau]$ to be $J_E\{0, \gamma_\tau 0\}(\tau)$, where γ_τ is a generator of the stabiliser Γ_τ of τ, suitably renormalised so as to have positive imaginary parts when viewed in $\mathcal{O}_\tau \subset K$.

Since K is imaginary quadratic, the unit group of $\mathcal{O}_\tau$ now has rank 0 so γ_τ — and hence $J_E[\tau]$ as well — is torsion. In fact, when τ has discriminant other than $D = -3, -4$, the unit group of $\mathcal{O}_\tau$ is trivial, which means that $\gamma_\tau = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $J_E[\tau] = 1$. Letting $\varepsilon_{-4} = i$ and $\varepsilon_{-3} = \frac{1}{2}(1 + i\sqrt{3})$, which correspond to $\varepsilon_{n^2-4} = \frac{1}{2}(n + \sqrt{n^2 - 4})$ for $n = 0, 1$, we find, as in Proposition 15,

$$\gamma_{-4} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad J_E[\varepsilon_{-4}] = \Phi_E(\varepsilon_{-4}),$$

$$\gamma_{-3} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \quad J_E[\varepsilon_{-3}] = \Phi_E(\varepsilon_{-3}).$$

Lemma 17. *If $(-4/p) = -1$, then $J_E[\varepsilon_{-4}] = \pm 1$, and if $(-3/p) = -1$, then $J_E[\varepsilon_{-3}]$ is a cube root of unity.*

Proof. The element γ_{-3} is 3-torsion so the same holds for $J_E[\varepsilon_{-3}]$. For the same reason, $J_E[\varepsilon_{-4}]$ is 4-torsion, but in fact, as $\gamma_{-4}^2 = -\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ fixes 0,

$$J_E[\varepsilon_{-4}]^2 = J_E\{0, \gamma_{-4}^2 0\}(\varepsilon_{-4}) = 1. \qquad \square$$

Remark 18. In concrete instances, it is not hard to determine when these "CM Stark–Heegner points" are trivial: this happens precisely when they are congruent to 1 modulo p, since the only torsion point in $\mathcal{O}_{\mathbb{C}_p}^\times$ congruent to 1 modulo p is 1. Experiments with curves of prime conductor of rank 0, 1 and 2 and conductor ≤ 2089 suggest that these points, in addition to being torsion, appear to always be trivial. This resonates with the philosophy that Stark–Heegner points ought to be defined over K when K has class number one, given that the rank two elliptic curves we have examined have trivial torsion over quadratic fields, (even if, of course, Conjecture 7(2) no longer holds in this setting).

It should be noted that the elements ε_D belong to the standard affinoid $\mathfrak{H}_p^\circ \subset \mathfrak{H}_p$ when p in inert in K_D. Corollary 16 suggests tackling Yokoi's conjecture by

studying the solutions of the equation

$$\Phi_E(z) = 1$$

that lie in the standard affinoid. The next section shows that this question can largely be reduced, thanks to Hensel's lemma, to a similar question for the mod p reduction of $\Phi_E(z)$ (more precisely, of its restriction to $\mathfrak{H}_p^\circ$), a rational function over the field with p elements.

5. Rational period functions

Let $X := \mathbb{P}_1 - \mathbb{P}_1(\mathbb{F}_p)$ be the "pointless" affine curve over $\mathbb{F}_p$ consisting of the complement of the $\mathbb{F}_p$-rational points in $\mathbb{P}_1$, and let

$$\mathcal{O}_X = \mathbb{F}_p[x][(x^p - x)^{-1}] \subset \mathbb{F}_p(x)$$

be its ring of regular functions. If $\mathrm{ord}_p(q) = 1$, then the function $\Phi_E \in \mathcal{O}^\times_{\mathfrak{H}_p}/q^{\mathbb{Z}}$ can be translated by a suitable power of q so that it maps the standard affinoid $\mathfrak{H}_p^\circ$ to $\mathcal{O}^\times_{\mathbb{C}_p} \subset \mathcal{O}_{\mathbb{C}_p}$. This representative belongs to the integral Tate algebra $\mathcal{O}^{\mathrm{int}}_{\mathfrak{H}_p^\circ} \subset \mathcal{O}_{\mathfrak{H}_p^\circ}$. Reduction modulo p gives rise to maps

$$\mathrm{red}_p : \mathfrak{H}_p^\circ \to X(\overline{\mathbb{F}}_p), \quad \mathrm{red}_p : \mathcal{O}^{\mathrm{int}}_{\mathfrak{H}_p^\circ} \to \mathcal{O}_X.$$

The image

$$R_E(x) := \mathrm{red}_p(\Phi_E|_{\mathfrak{H}_p^\circ}) \in \mathcal{O}_X^\times$$

of Φ_E is called the (mod p) *rational period function* attached to E.

The following is a direct consequence of Hensel's lemma:

Lemma 19. *Let $x \in X(\overline{\mathbb{F}}_p)$ be a solution of the equation $R_E(x) = 1$ for which $R'_E(x) \neq 0$. Then there is a unique $z \in \mathfrak{H}_p^\circ$ satisfying*

$$\mathrm{red}_p(z) = x, \quad \Phi_E(z) = 1.$$

We obtain the following corollary:

Corollary 20. *Let E be an elliptic curve of prime conductor p and rank ≥ 2 over $\mathbb{Q}$ having no quadratic torsion. Assuming Conjecture 7, $R_E(\varepsilon_D) = 1$ for all discriminants $D = n^2 \pm 4$ of class number one in which p is inert. If ε_D is a simple zero of $R_E(x) - 1$, then ε_D is the only solution to $\Phi_E(\tau) = 1$ in its mod p residue disc.*

Corollary 20 reduces the study of Yokoi's conjecture to the determination of the zeroes of a single rational function over $\mathbb{F}_p$, the function $R_E(x) - 1$. We now proceed to give an explicit formula for $R_E(x)$ which allows it to be calculated efficiently on the computer.

This formula depends on the even $\Gamma_0(p)$-invariant modular symbol

$$m_E\{r, s\} := \frac{1}{\Omega_E^+} \mathrm{Re}\left(\int_r^s 2\pi i f_E(z)\, dz \right) \in \mathbb{Z}$$

attached to E, and on the associated *Manin symbol*

$$M_E : \mathbb{P}_1(\mathbb{F}_p) \to \mathbb{Z}$$

defined by

$$M_E(a) := \begin{cases} m_E\{a/p, \infty\} & \text{if } a = 0, 1, \ldots, p-1, \\ -m_E\{0, \infty\} & \text{if } a = \infty. \end{cases}$$

The value $M_E(0)$ is a nonzero multiple of $L(E, 1)$ and hence vanishes when E has analytic rank ≥ 1. The following proposition examines the $\mathrm{GL}_2(\mathbb{Z})$-invariant modular symbol

$$\bar{J}_E : \mathbb{P}_1(\mathbb{Q}) \times \mathbb{P}_1(\mathbb{Q}) \to \mathcal{O}_X^\times$$

defined by

$$\bar{J}_E\{r, s\} = \mathrm{red}_p(J_E\{r, s\}|_{\mathfrak{H}_p^\circ}).$$

Proposition 21. *For all $r, s \in \mathbb{P}_1(\mathbb{Q})$,*

$$\bar{J}_E\{r, s\} = \prod_{a \in \mathbb{F}_p} (z - a)^{M_{rs}(a)} \pmod{\mathbb{F}_p^\times}, \tag{19}$$

where

$$M_{rs}(a) := m_E\left\{\frac{r-a}{p}, \frac{s-a}{p}\right\}.$$

Proof. Let us first quickly recall the construction of the Γ-invariant elliptic modular symbol J_E. Let $\mathcal{D}(\mathbb{P}_1(\mathbb{Q}_p), \mathbb{Z})$ denote the space of *$\mathbb{Z}$-valued measures of total mass zero* on $\mathbb{P}_1(\mathbb{Q}_p)$, that is, the space of measures μ on the topological space $\mathbb{P}_1(\mathbb{Q}_p)$ for which $\mu(U) \in \mathbb{Z}$ for any compact-open subset U and $\mu(\mathbb{P}_1(\mathbb{Q}_p)) = 0$. If $\mu \in \mathcal{D}(\mathbb{P}_1(\mathbb{Q}_p), \mathbb{Z})$ is such a $\mathbb{Z}$-valued measure, we may define a multiplicative integral by considering Riemann products instead of Riemann sums: for any continuous $f : \mathbb{P}_1(\mathbb{Q}_p) \to \mathbb{C}_p^\times$,

$$\int\!\!\!\!\!\!\diagup_{\mathbb{P}_1(\mathbb{Q}_p)} f(t)\, d\mu(t) := \lim_{\mathbb{P}_1(\mathbb{Q}_p) = \{U_\alpha\}} \prod_\alpha f(t_\alpha)^{\mu(U_\alpha)},$$

where the limit is taken over finer and finer coverings of $\mathbb{P}_1(\mathbb{Q}_p)$ by mutually disjoint compact open subsets U_α and $t_\alpha \in U_\alpha$ is a sample point.

It is proved in [14, Section 1.2] that the even modular symbol m_E may be upgraded uniquely to an even modular symbol

$$\mu_E : \mathbb{P}_1(\mathbb{Q}) \times \mathbb{P}_1(\mathbb{Q}) \to \mathcal{D}(\mathbb{P}_1(\mathbb{Q}_p), \mathbb{Z})$$

satisfying

$$\mu_E\{r, s\}(\mathbb{Z}_p) = m_E\{r, s\}, \quad \mu_E\{\gamma r, \gamma s\}(\gamma U) = \mu_E\{r, s\}(U)$$

for all $r, s \in \mathbb{P}_1(\mathbb{Q})$ and $\gamma \in \mathrm{GL}_2(\mathbb{Z})$. For simplicity and to avoid the $q^{\mathbb{Z}}$ ambiguity, we now restrict ourselves to the standard affinoid $\mathfrak{H}_p^\circ$. Using this modular symbol,

we define a multiplicative line integral: for all $\tau_0, \tau \in \mathfrak{H}_p^\circ$ and $r, s \in \mathbb{P}_1(\mathbb{Q})$,

$$\fint_{\tau_0}^{\tau} \int_r^s \omega_E := \fint_{\mathbb{P}_1(\mathbb{Q}_p)} \left(\frac{\tau - t}{\tau_0 - t} \right) d\mu_E\{r, s\}(t). \tag{20}$$

The elliptic modular symbol J_E corresponds to the unique *indefinite integral*

$$J_E\{r, s\}(\tau) = \fint_{}^{\tau} \int_r^s \omega_E,$$

a Γ-invariant modular symbol with values in $\mathcal{O}_{\mathfrak{H}_p}^\times / q^{\mathbb{Z}}$ satisfying

$$\fint_{}^{\tau} \int_r^s \omega_E \div \fint_{}^{\tau_0} \int_r^s \omega_E = \fint_{\tau_0}^{\tau} \int_r^s \omega_E \tag{21}$$

for all $\tau_0, \tau \in \mathfrak{H}_p^\circ$ and $r, s \in \mathbb{P}_1(\mathbb{Q}_p)$. (See [14, Section 3.3].) Restricting J_E to $\mathfrak{H}_p^\circ$ and translating it by a suitable power of q, it becomes a $\mathrm{GL}_2(\mathbb{Z})$-invariant modular symbol with values in $(\mathcal{O}_{\mathfrak{H}_p^\circ}^{\mathrm{int}})^\times$. For all $a \in \mathbb{P}_1(\mathbb{F}_p)$, let

$$B_a = \begin{cases} a + p\mathbb{Z}_p & \text{if } a \neq \infty, \\ \mathbb{P}_1(\mathbb{Q}_p) \setminus \mathbb{Z}_p & \text{if } a = \infty \end{cases}$$

denote the preimage of $\{a\}$ under the reduction map $\mathbb{P}_1(\mathbb{Q}_p) \to \mathbb{P}_1(\mathbb{F}_p)$. We can then write $B_a = \gamma_a \mathbb{Z}_p$, where

$$\gamma_a = \begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix} \quad \text{if } a \neq \infty, \qquad \gamma_a = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix} \quad \text{if } a = \infty.$$

For all $r, s \in \mathbb{P}_1(\mathbb{Q}_p)$ and any $a = 0, 1, \ldots, p-1$, one finds that

$$\mu_E\{r, s\}(B_a) = \mu_E\{\gamma_a^{-1} r, \gamma_a^{-1} s\}(\mathbb{Z}_p) = m_E \left\{ \frac{r-a}{p}, \frac{s-a}{p} \right\} = M_{rs}(a).$$

The divisor of $\bar{J}_E\{r, s\}(\tau)$ is the same as that of the image under red_p of the function in (20), where τ_0 is an arbitrary base point in $\mathfrak{H}_p^\circ$ and τ is treated as the variable. This divisor is equal to

$$\mathrm{Div}(\bar{J}_E\{r, s\}) = \sum_{a \in \mathbb{P}_1(\mathbb{F}_p)} M_{rs}(a)\langle a \rangle,$$

where

$$M_{rs}(\infty) = -M_{rs}(0) - \cdots - M_{rs}(p-1).$$

Proposition 21 follows directly since the rational function on the right of (19) has the same divisor. □

By specialising this proposition to $(r, s) = (0, \infty)$, since m_E is even, we obtain:

Corollary 22. *The rational period function $R_E(x)$ satisfies*

$$R_E(x) = \prod_{a \in \mathbb{F}_p} (x - a)^{M_E(a)} \pmod{\mathbb{F}_p^\times}.$$

Corollary 22 already suffices to compute the rational period function $R_E(x)$ in practice, since the three-term relation can be used to identify the correct constant. It is however possible to give a simple closed formula for $R_E(x)$ in all cases.

Proposition 23. *The rational period function $R_E(x)$ is given by*

$$R_E(x) = x^{M_E(0)} \times \prod_{M_E(a)>0} (x-a)^{M_E(a)} \times \prod_{M_E(a)<0} \left(1-\frac{x}{a}\right)^{M_E(a)}, \tag{22}$$

where the products are taken over the $a \in \mathbb{F}_p^\times$.

Proof. Corollary 22 shows that (22) is true up to a multiplicative scalar. To check that this scalar is trivial, it suffices to verify that the formula for $R_E(x)$ in (22) satisfies the two- and three-term identities of (17) which $R_E(x)$ inherits from the rigid analytic period function $\Phi_E(z)$. Set

$$c = \prod_{M(a)<0} (-a)^{M(a)} = \prod_{M(a)<0} a^{M(a)} \quad \text{and} \quad R(z) = \prod_{a\in\mathbb{F}_p} (z-a)^{M(a)}$$

(since M is even) so that the right-hand side of (22) is $c^{-1}R$. After computing the first nonzero Laurent coefficients at 0 of

$$R\left(\frac{1}{z}\right) = z^{-M(0)} \prod_{a\in\mathbb{F}_p^\times} z^{-M(a)}(1-az)^{M(a)},$$

$$R\left(\frac{z+1}{z}\right) = z^{-M(0)}(z+1)^{M(0)} \prod_{a\in\mathbb{F}_p^\times} z^{-M(a)}(z+1-az)^{M(a)},$$

$$R(z+1) = z^{M(1)} \prod_{a\in\mathbb{F}_p^\times} (z-a)^{M(a+1)},$$

we see that the two- and three-term relations

$$R_E(x)R_E\left(\frac{1}{x}\right) = 1 \quad \text{and} \quad R_E\left(\frac{x+1}{x}\right)R_E(x) = R_E(x+1)$$

amount to

$$\prod_{a\in\mathbb{F}_p^\times} a^{M(a)} \times 1 = c^2 \quad \text{and} \quad 1 \times \prod_{a\in\mathbb{F}_p^\times} a^{M(a)} = c \times \prod_{a\in\mathbb{F}_p^\times} a^{M(a+1)},$$

respectively. The first equality follows from the observation that

$$c = \prod_{M(a)>0} a^{M(a)} = \prod_{M(b)<0} b^{M(b)},$$

as seen by letting $b = 1/a$ and recalling that $M(1/a) = -M(a)$, and the second by grouping together a with $1/a$ on the right-hand side and recalling that $M(a+1) - M(1/a+1) = M(a)$. □

Remark 24. When E has rank at least two, the simpler formula

$$R_E(x) = \prod_{a=1}^{p-1} (x-a)^{M_E(a)} \tag{23}$$

seems to hold. To show this we need to prove the triviality of the scalar $c = \prod_{M(a)>a} a^{M(a)}$, whose square is

$$\Omega_{\mathrm{MT}}(E) := \prod_{a=1}^{p-1} a^{M_E(a)} \in \mathbb{F}_p^\times.$$

This interesting quantity arises as the "first derivative" of the "theta element"

$$\theta_E := \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} M_E(a) \cdot \langle a \rangle \in \mathbb{Z}[(\mathbb{Z}/p\mathbb{Z})^\times]$$

attached to E, an object that belongs to the integral group ring of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ and can be viewed as a tame refinement of the Mazur–Swinnerton-Dyer p-adic L-function attached to E. This tame refinement is studied in [23], where it is conjectured that it belongs to the r-th power if the augmentation ideal in the integral group ring, where r is the rank of $E/\mathbb{Q}$, and even to its $(r+1)$-st power when E has split multiplicative reduction at p. The quantity $\Omega_{MT}(E)$ encodes the image of θ_E in I/I^2 and hence is predicted to be equal to 1 when $r \geq 2$. This is essentially proved in [31], which gives strong evidence towards the Mazur–Tate conjecture building on the p-adic insights of Greenberg and Stevens. The fact that the scalar c, a canonical square root of $\Omega_{MT}(E)$, is also equal to 1 appears to be a slight but nontrivial refinement of the Mazur–Tate conjecture in this setting.

6. Yokoi's conjecture

We are now ready to prove the main theorem of the introduction concerning the conjectures of Yokoi and Mollin:

Theorem 25. *Assume Conjecture 7 of Section 3. Then the class number one discriminants of the form* n^2+4 *are equal to* 5, 8, 13, 20, 29, 53, 68, 125, 173, *or* 293, *and those of the form* n^2-4 *are equal to* -4, -3, 5, 12, 21, 32, 45, 77, 117, *or* 437.

Proof. The elliptic curve of rank two and smallest prime conductor is the curve denoted by $E = 389A1$ in the tables of Cremona [13], with equation given by

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

A computer calculation shows that the rational period function $R_E(x)$ has degree 144, and the numerator of the rational function $R_E(x) - 1$, a polynomial of degree 142, factors into:

• 66 linear factors, with roots 0 (twice), ± 1 (three times), ± 2 (twice), $\pm\frac{1}{2}$ (twice), ± 115 (once), and twelve quadruples of roots of the form $a, -a, 1/a, -1/a$ with

$$a = 3,\ 4,\ 6,\ 10,\ 13,\ 15,\ 62,\ 98,\ 101,\ 117,\ 123,\ \tfrac{2}{3}.$$

• 6 quadratic factors of the form $x^2 \pm nx - 1$, with $n = 2, 5, 7$, corresponding to the discriminants $D = 8, 29$, and 53 in (5). These are precisely the discriminants in (5) which are not quadratic residues modulo 389. This proves that any class number one discriminant of the form $n^2 + 4$ with $n > 391$ must be divisible by 389.

• 10 quadratic factors of the form $x^2 \pm nx + 1$, with $n = 1, 4, 5, 6, 21$, corresponding to the discriminants $D = -3, 12, 21, 32$, and 437 in (6). The integers in this list are precisely the discriminants in (6) which are not quadratic residues modulo 389. The fact that Φ_E vanishes at the roots of the polynomials $x^2 \pm x + 1$ can be deduced directly from Lemma 17, by observing that the vanishing of $R_E(x) - 1$ at ε_{-3} means that $J_E[\varepsilon_{-3}]$ is congruent to 1 modulo p, and so is equal to 1 since the only such torsion point in $\mathcal{O}_{\mathbb{C}_p}^\times$ is 1. This proves that any class number one discriminant of the form $n^2 - 4$ with $n > 391$ must be divisible by 389.

• 4 irreducible factors of degree 11, namely,

$$h(x) = x^{11} + 61x^{10} - 192x^9 + 134x^8 + 19x^7 - 80x^6 + 66x^5 + 64x^4 + 48x^3 - 159x^2 - 50x - 70,$$

along with $h(-x)$, $x^{11}h(1/x)$, and $x^{11}h(-1/x)$.

The factorisation of $R_E(x) - 1$ shows that the equation $\Phi_E(\tau) = 1$ has exactly 76 solutions in $\mathfrak{H}_{389}^\circ$. Four of these are the CM points of the form $\pm\varepsilon_{-3}$ and $\pm\varepsilon_{-3}^{-1}$. Assuming Conjecture 7 and the attendant Corollary 16, there are 28 further roots given by the RM points

$$\pm 1 \pm \sqrt{2}, \quad \tfrac{1}{2}(\pm 5 \pm \sqrt{29}), \quad \tfrac{1}{2}(\pm 7 \pm \sqrt{53}), \quad \pm 2 \pm \sqrt{3},$$
$$\tfrac{1}{2}(\pm 5 \pm \sqrt{21}), \quad \pm 3 \pm 2\sqrt{2}, \quad \text{and} \quad \tfrac{1}{2}(\pm 21 \pm \sqrt{437}).$$

Finally, $\Phi_E(\tau) - 1$ vanishes at 44 presumably transcendental elements of the unramified extension of $\mathbb{Q}_{389}$ of degree 11.

A similar computer calculation with the elliptic curve $433A1$ of conductor 433 leads to the conclusion that any class number one discriminant of the form $n^2 \pm 4$ not listed in Theorem 25 must also be divisible by 433. By the main theorem of genus theory, the genus field of K_D contains both $\sqrt{433}$ and $\sqrt{389}$, contradicting the class number one assumption on D. Theorem 25 follows. □

The factorisation of $R_E(x) - 1$ for the curves $389A1$ and $433A1$ is summarised in the first two lines of Table 1, in which similar data is gathered for all the elliptic curves of analytic rank two of prime conductor ≤ 1000, as well as for the elliptic

curve $5077A1$ of smallest prime conductor and rank 3, which plays such a key role in the work of Goldfeld–Gross–Zagier.

The first column of Table 1 gives the label for the elliptic curve E of rank ≥ 2 following the conventions of Cremona. (The reader is cautioned that these sometimes differ from the ones in the LMFDB.) The second column gives the degree of the rational function $R_E(x)$, which in all cases provides a (strict) upper bound for the number of solutions to $\Phi_E(z) = 1$ in $\mathfrak{H}_p^\circ$. The third column indicates the number of elements of $\mathbb{P}_1(\mathbb{F}_p)$ that occur (with multiplicity) in the fiber of $R_E(x)$ above $x = 1$, which is always less than the degree of $R_E(x)$.

The integers in the fourth and fifth columns of Table 1 that are printed in a regular font correspond to class number one discriminants in the lists (5) and (6) respectively. Those in boldface correspond to discriminants with larger class numbers, but for which we are nevertheless able to predict that the associated Stark–Heegner point vanishes because of "excess vanishing" of suitable twisted L-series of E, as will be explained in more detail shortly. The integers with a superscript of ? indicate more problematic mod p roots which do not seem to correspond to a Stark–Heegner point of finite order. It is then entirely possible that the solutions of $\Phi_E(z) = 1$ in the associated residue discs of $\mathfrak{H}_p^\circ$, although quadratic over $\mathbb{Q}_p$, are not RM points and are likely to be transcendental over $\mathbb{Q}$. When such "parasitic factors" occur in the factorisation of $R_E(x) - 1$, they present a more serious obstruction to parlaying E into a proof of Theorem 25.

Finally, the last column of Table 1 lists the degrees of the irreducible factors of the numerator of $R_E(x) - 1$ that are not of the form $x^2 \pm nx \pm 1$.

We now turn to a discussion of some of the integers that appear in boldface in the fourth and fifth columns of Table 1. They correspond to factors of $R_E(x) - 1$ of the form $x^2 + nx \pm 1$, where n is small but $D = n^2 \mp 4$ does not have class number one. These factors, while seemingly not accounted for by Conjecture 7, are sometimes explained by a *twisted* version of the Gross–Zagier formula of Conjecture 7 formulated in [14, Conjecture 5.15] (some cases of which were proven in a weaker form, when χ is a genus character, in [22], building on [5] and [25]):

Conjecture 26. *Let $\tau \in \mathfrak{H}_p^{\mathrm{RM}}$ be an RM point with associated order $\mathcal{O}_\tau = \mathcal{O}_D$ and let $P = J_E[\tau]$ be the associated Stark–Heegner point in $E(H_D)$. If χ is any primitive character of $\mathrm{Cl}(D) \simeq \mathrm{Gal}(H_D/K_D)$, then*

$$\mathrm{ht}_E(P(\chi)) \sim L'(E/K, \chi, 1),$$

where

$$P(\chi) := \sum_{\sigma \in \mathrm{Gal}(H_D/K_D)} \overline{\chi}(\sigma) P^\sigma \in (E(H_D) \otimes \mathbb{C})(\chi)$$

is the χ-isotypical component of P.

E	$\deg(R_E)$	linear factors	$x^2 \pm nx - 1$	$x^2 \pm nx + 1$	degrees of other factors
$389A1$	144	66	2, 5, 7	1, 4, 5, 6, 21	11^4
$433A1$	162	60	1, 4, 5, 11, 13	3, 5, 7, 9	$5^4 10^2 12^2$
$563A1$	152	64	1, 2, 4, 5, 7, 11 13, 17, **31**, **41**	0, 1, 3, 6, 7	$2^2 6^4$
$571B1$	204	84	2, 7, 8	0, 4, 6, 9, 21, **31**	$2^2 6^2 7^4 10^4$
$643A1$	180	56	1, 2, 3, 4, 8, 11	0, 3, 4, 5, 6, 7, 9 11, 21, **33**, $160^?$	$4^6 16^2$
$709A1$	296	70	2, 3, 7, 8, 13, **16**	6, 11, 21, **24**	$10^4 22^2 24^2 26^2$
$997B1$	460	54	1, 2, 4, 5, 8 11, 17, $64^?$	3, 5, 6, 7	$2^6 4^2 168^2$
$997C1$	328	72	1, 2, 4, 5, 8 11, **16**, 17, **31** **53**, $380^?$, $463^?$	3, 5, 6, 7, **17**	$2^6 8^4 72^2$
$5077A1$	4624	56	1, 2, 3, 4, 5, 8, 11	3, 6, 7, 9, 11, 21, $956^?$, $2000^?$	$2^4 4^2 8^2 24^2 49^4$ $70^2 72^2 274^2$ $358^2 1342^2$

Table 1. Factorisation of $R_E(x) - 1$.

Conjecture 26 predicts that the Stark–Heegner point P is torsion whenever

$$L'(E/K_D, \chi, 1) = 0 \quad \text{for every character } \chi \text{ of } \mathrm{Cl}(D).$$

When $\mathrm{Cl}(D)$ is an elementary 2-group, i.e., every form of discriminant D is ambiguous, all the characters of $\mathrm{Cl}(D)$ are quadratic and described by genus theory in terms of Kronecker symbols $\left(\frac{d}{\cdot}\right)$ for some $d \mid D$. (See [12, Theorem 18.27].) In this case, up to finitely many Euler factors,

$$L(E/K_D, \chi, s) = L(E^{(d)}/\mathbb{Q}, s) \cdot L(E^{(D/d)}/\mathbb{Q}, s)$$

and its order of vanishing is the sum of the analytic ranks of the quadratic twists $E^{(d)}$ and $E^{(D/d)}$ of E.

For example, consider the elliptic curve of rank 2 and conductor $p = 563$, labelled $563A1$ in Cremona's tables. When factoring the numerator of $R_E(x) - 1$ over $\mathbb{F}_p[x]$, we obtain the quadratic factors $x^2 + 31x - 1$ and $x^2 + 41x - 1$ corresponding to the discriminants

$$D_1 = 31^2 + 4 = 5 \cdot 193 \quad \text{and} \quad D_2 = 41^2 + 4 = 5 \cdot 521$$

of class number 2. For each of $j = 1, 2$, the nontrivial character of $\mathrm{Cl}(D_j)$ cuts out the extension of K_D generated by $\sqrt{5}$. It turns out that $E^{(5)}$ has rank 2 and hence that $L'(E^{(5)}/\mathbb{Q}, 1) = 0$. Conjecture 26 therefore implies that all the χ-components of P are trivial, hence this Stark–Heegner point is torsion. Since it is moreover congruent to 1 modulo p, it must correspond to an actual zero of $\Phi_E - 1$.

Remark 27. It may appear somewhat surprising that the fiber $R_E^{-1}(1)$ has so many $\mathbb{F}_p$-rational elements while $R_E(x)$ itself already has all its zeros and poles in $\mathbb{P}_1(\mathbb{F}_p)$. Such zeros do not lift to the standard affinoid $\mathfrak{H}_p^\circ$, reflecting the fact that the equation $\Phi_E(\tau) = 1$ has fewer solutions in $\mathfrak{H}_p^\circ$ than the equation $\Phi_E(\tau) = t$ for all but finitely many t. This phenomenon seems to fall outside the framework of real multiplication. The authors have checked that this pattern persists for all curves of rank ≥ 2 and conductor less than 10000. Moreover, for curves of rank 2, the elements 0, 1, 2, 3, 4, 6, $\frac{2}{3}$ and $\frac{3}{4}$ seem to always be roots of $R_E(x) - 1$ with respective multiplicities 2, 3, 2, 1, 1, 1 and 1. These also seem to be the only critical points of $R_E(x) - 1$, i.e., roots with multiplicity ≥ 2.

For elliptic curves of rank 1, the pattern breaks down and $R_E(x) - 1$ has almost no $\mathbb{F}_p$-rational zeros, never exceeding 18 such roots. We checked that 1 and -1 were always, for curves of conductor ≤ 2089 which are unique in their isogeny class, in the fiber of 1 with multiplicity 3, as well as ∞ with multiplicity 2. Again, these appear to be the only critical points. Sometimes there are no other $\mathbb{F}_p$-rational zeros.

For curves of rank 0 and conductor ≤ 2089 which are unique in their isogeny class, $R_E(x) - 1$ always has 1 and -1 as simple roots as well as ∞ with multiplicity 2. The only critical point is ∞. Most of the time it has few rational zeros (at most 18), sometimes it has no other rational zeros, sometimes it has around 50. This is for instance the case for the elliptic curve with LMFDB label $1171B1$.

7. Chowla's conjecture

This section explains how similar ideas can be adapted to yield a (conditional) proof of Chowla's conjecture:

Theorem 28. *Assume Conjecture 7 of Section 3. Then the class number one discriminants of the form* $4n^2 + 1$ *are equal to* 5, 17, 37, 101, 197, *or* 677.

To explain how the approach of the previous section can be adapted to also yield Theorem 28, it is convenient to first work in a greater generality.

Let $D > 0$ be any positive discriminant, $\mathcal{O}_D$ the quadratic order of discriminant D, and $\varepsilon_D = u + v\frac{1}{2}\sqrt{D}$ its fundamental unit. The stabiliser of a primitive binary form $Q = ax^2 + bxy + cy^2$ of discriminant D is generated by

$$\gamma_Q = \begin{pmatrix} u - \frac{1}{2}bv & -cv \\ av & u + \frac{1}{2}bv \end{pmatrix}.$$

In particular, $\gamma_Q\infty$ has denominator av. Let ρ be the matrix $\left(\begin{smallmatrix}1 & w\\ 0 & av\end{smallmatrix}\right)$ with $w = u - \frac{1}{2}bv$. If τ_Q denotes a root of $Q(x, 1)$, the fundamental automorph of τ_Q is (up to sign) $\gamma_Q^{\pm 1}$ and we have

$$J_E[\tau_Q]^{\pm 1} = J_E\{\infty, \gamma_{\tau_Q}\infty\}(\tau_Q) = J_E\{\rho\infty, \rho 0\}(\tau_Q).$$

Putting $\rho = \left(\begin{smallmatrix}1 & q\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & r\\ 0 & av\end{smallmatrix}\right)$ in Hermite normal form, we end up with

$$J_E[\tau_Q]^{\pm 1} = J_E\left\{\infty, \frac{r}{av}\right\}(\tau_Q - q),$$

where $w = qav + r$ is the Euclidean division of w by av. This suggests trying to enumerate real quadratic fields of class number one based on the "quadratic part" v, i.e., the conductor of the order $\mathbb{Z}[\varepsilon_D]$ generated by the fundamental unit. Indeed, fixing v and letting Q be the principal form (which has $a = 1$), we see that $J_E[\tau_Q]$ can be written as the evaluation of some function j at some translate of τ_Q, where j belongs to the finite set of functions of the form $J_E\{r/v, \infty\}^{\pm 1}$ for some integer $0 \le r < v$.

Proposition 29. *Let $Q = ax^2 + bxy + cy^2$ be a primitive binary form of discriminant $D > 0$ and let τ_Q be a root of $Q(x, 1)$. Let ε_D be the fundamental unit of $\mathcal{O}_D$ and let v be the conductor of the order $\mathbb{Z}[\varepsilon_D]$. Then there exist integers $0 \le r < av$ and $q \in \mathbb{Z}$ such that* $\gcd(r, av) = 1$ *and*

$$J_E[\tau_Q]^{\pm 1} = J_E\left\{\frac{r}{av}, \infty\right\}(\tau_Q - q),$$

where the ± 1 sign depends on the chosen root of $Q(x, 1)$.

Proof. We have proved everything except that $r \equiv u - \frac{1}{2}bv \pmod{av}$ is coprime to av, which follows from the equality

$$\left(u - \tfrac{1}{2}bv\right)\left(u + \tfrac{1}{2}bv\right) + (av)(cv) = \det\rho = \pm 1. \qquad \square$$

In Section 6, we studied discriminants D for which the conductor is 1, corresponding to $D = n^2 \pm 4$. We now proceed to do the same when the conductor is 2, this time corresponding to the families $D = 4n^2 + 1$ and $D = 4(n^2 - n)$. Indeed, the order $\mathcal{O}_D$ contains the small unit $\varepsilon_D := 2n + \sqrt{D}$ when $D = 4n^2 + 1$ and $\varepsilon_D := (2n - 1) + \sqrt{D}$ when $D = 4(n^2 - n)$.

Proof of Theorem 28. Just as $D = 5$ both had the form $n^2 + 4$ and $n^2 - 4$, the small unit ε_D need not be fundamental but merely a power of the fundamental unit. (In fact it is either the fundamental unit or its square.) Let

$$\alpha_D = \begin{cases} \frac{1}{2}(-2n - 1 + \sqrt{4n^2 + 1}) & \text{if } D = 4n^2 + 1, \\ -n + \sqrt{n^2 - n} & \text{if } D = 4(n^2 - n) \end{cases}$$

be a root of $x^2 + (2n + 1)x + n$ in the former case and $x^2 + 2nx + n$ in the latter.

Making Proposition 29 explicit for those families, we obtain:

Corollary 30. *Let $D>0$ have the form $4n^2+1$ or $4(n^2-n)$ and let $\tau_D=\frac{1}{2}(D+\sqrt{D})$. Then a power of $J_E[\tau_D]$ is equal to $J_E\{-\frac{1}{2},\infty\}(\alpha_D)$.*

Corollaries 30 and 11 invite us to examine the quadratic factors in the factorisation of $R_E^{(2)}(x)-1$, where

$$R_E^{(t)}(x)=\mathrm{red}_p(J_E\{-1/t,\infty\}|_{\mathfrak{H}_p^\circ}).$$

As in the study of Yokoi's conjecture, Table 2 summarises the factorisation of the numerator of the rational function $R_E^{(2)}(x)-1$, following the same conventions as in Table 1. The second and third lines of this table, corresponding to the elliptic curves $433A1$ and $563A1$ respectively, imply that any class number one discriminant of the form $4n^2+1$ outside of the list in Theorem 28 must be divisible by the two primes 433 and 563, contradicting genus theory. □

As a byproduct of the proof of Theorem 28 and the data gathered in Table 2, we also deduce the following list of class number one discriminants of the form $4(n^2-n)$:

Corollary 31. *Assuming Conjecture 7 and its twisted variant, Conjecture 26, there are exactly four discriminants of the form $D=4(n^2-n)$ with class number one*:

$$D=8,\ 24,\ 48,\ 80.$$

Let us now discuss further some of the outcomes of the numerical experiments summarised in Table 2. For the unique elliptic curve E of rank 2 and conductor $p=389$ labelled $389A1$ in Cremona's tables, the quadratic factors of $R_E^{(2)}(x)-1$ turn out to be

$$2x^2-1,\quad 2x^2-2x-1,\quad x^2+7x+3,\quad x^2+11x+5,\quad x^2+15x+7$$
$$x^2+27x+13,\quad x^2+59x+29,\quad x^2+4x+2,\quad x^2+8x+4,\quad x^2+20x+10,$$

as well as their images by the matrix $\left(\begin{smallmatrix}-1&-1\\0&1\end{smallmatrix}\right)$, which exchanges $-\frac{1}{2}$ and ∞. All of these are as predicted by Proposition 29: the first two factors corresponding to $a=2$ and $v=1$, and the rest to $a=1$ and $v=2$. Each of the discriminants of these quadratic polynomials has class number one, apart from $x^2+59x+29$ and $x^2+20x+10$, whose discriminants 3365 and 360 both have class number two.

In the case where $D=3365=5\cdot 673=4\cdot 29^2+1$, one computes that the Hasse–Weil L-function of E/K_D twisted by the nontrivial character χ of $\mathrm{Cl}(D)$,

$$L(E/K_D,\chi,s)=L(E^{(5)},s)\cdot L(E^{(673)},s),$$

vanishes to order 3 at $s=1$ because of a double zero in the first factor. As explained in Section 6, this is enough to imply the triviality of the Stark–Heegner point of discriminant D on E, assuming Conjecture 26.

In the case where $D = 360 = 2^3 \cdot 3^2 \cdot 5$, the order $\mathcal{O}_D$ is nonmaximal and has conductor 3 in the maximal order $\mathbb{Z}[\sqrt{10}]$ of discriminant 40. Letting χ be the nontrivial character of $\mathrm{Cl}(360) = \mathrm{Cl}(40)$, the χ-component, denoted by $P_{40}(\chi) \in E(H_{40})$, of the Stark–Heegner point of discriminant 40 appears to be nontrivial, and indeed the twisted Hasse–Weil L-function

$$L(E/K_{40}, \chi, s) = L(E^{(5)}/K_{40}, s)$$

vanishes to order 1 at $s = 1$. The Stark–Heegner point $P_{360}(\chi)$ is defined over the same field as $P_{40}(\chi)$ since $H_{360} = H_{40}$, however, the two points are not the same. Rather, the norm-compatibility property (15) satisfied by the Stark–Heegner points shows that

$$P_{360}(\chi) = (a_3(E) - \chi(\mathfrak{p}_3) - \chi(\bar{\mathfrak{p}}_3))P_{40}(\chi),$$

where $a_3(E)$ is the third Fourier coefficient of the cusp form attached to E, and $\mathfrak{p}_3$ and $\bar{\mathfrak{p}}_3$ are the two prime ideals of $\mathbb{Z}[\sqrt{10}]$ above 3. Since these primes are inert in H_{40}/K_{40}, we have $\chi(\mathfrak{p}_3) = \chi(\bar{\mathfrak{p}}_3) = -1$, and one verifies that $a_3(E) = -2$. It follows that $P_{360}(\chi) = 0$ because of the presence of this local factor at the prime 3, even though $P_{40}(\chi)$ turns out to be nontrivial. Since the trace $P_{360}(1)$ of the Stark–Heegner point P_{360} is also torsion, it follows that P_{360} is itself a point of finite order, as suggested by the experiment.

The integer denoted by $37^?$ in the row attached to the elliptic curve $E = 571B1$ in Table 2 corresponds to the prime discriminant $D = 4 \cdot 37^2 + 1 = 5477$ of class number three. This suggests that the Hasse–Weil L-series of E over K_D twisted by any cubic unramified character χ of K_D might vanish to order ≥ 3. We thank one of the referees for verifying that the first and second derivatives of these L-series at the central point are very small and hence ostensibly zero, by a calculation in `magma` that would have taxed the authors' computational expertise. While the numerics are convincing, the conjectural nature of the Gross–Zagier formula for Stark–Heegner points places a rigorous proof of the vanishing of $L'(E/K_D, \chi, 1)$ squarely beyond the reach of machine calculations.

Remark 32. The method we have described seems to apply to families of discriminants D whose fundamental unit $\varepsilon_D = u_D + v_D \frac{1}{2}\sqrt{D}$ has quadratic part v_D bounded by some fixed v. For instance, the family $D = n^2 + 2$, whose fundamental unit is given by

$$\varepsilon_D = (n^2 + 1) + n\sqrt{n^2 + 2}$$

lies ostensibly outside of the scope of the method even though its regulator has size $O(\log(D))$. It would be interesting to further probe the limits of the "Stark–Heegner approach" by trying to extend it to more general families of real quadratic fields of Richaud–Degert type.

E	$\deg(R_E^{(2)})$	linear factors	$x^2+(2n+1)x+n$	$x^2+2nx+n$	degrees of other factors
$389A1$	166	36	$\frac{1}{2}$, 3, 5, 7, 13, **29**	$\frac{3}{2}$, 2, 4, **10**	44^2
$433A1$	194	44	1, 5, 13	5, **10**	$2^2 18^2 44^2$
$563A1$	176	48	$\frac{1}{2}$, 1, 3, 13	$\frac{1}{2}$, 2, 3, 5, **7**	$4^2 42^2$
$571B1$	208	48	$\frac{1}{2}$, 2, 5, 7, **23**, **29**, $37^?$	$\frac{1}{2}$, $\frac{3}{2}$, 2, 4 **10**, **12**	$4^2 25^4$
$643A1$	188	40	$\frac{1}{2}$, 1, 2, 3, 7, 11	$\frac{1}{2}$, $\frac{3}{2}$, 2, 4 5, **11**, **17**	$6^4 36^2$
$709A1$	338	52	$\frac{1}{2}$, 2, 3, 5, 7, 13	2, 3, $\frac{\mathbf{13}}{\mathbf{2}}$	$2^4 3^4 4^4 10^2 94^2$
$997B1$	494	32	$\frac{1}{2}$, 1, 2, 3, 7, 13	2, 3, 5	$4^2 12^2 17^4 22^2$ $26^2 32^2 82^2$
$997C1$	354	40	$\frac{1}{2}$, 1, 2, 3, 7, **11**, 13	2, 3, 5	68^4
$5077A1$	4852	30	$\frac{1}{2}$, 1, 2, 3, 5, 7, 13	2, 3, 5, **9**	$2^2 26^2 32^2 67^4$ $75^4 101^4 110^2$ $151^4 178^4 336^2$ $346^2 394^2$

Table 2. Factorisation of $R_E^{(2)}(x)-1$.

Appendix: Computer code

The following SageMath code computes the rational function $R_E(x)$ as a function of the elliptic curve E:

```
def rational_period_function(E):
  p = E.conductor()
  Poly.<z> = PolynomialRing(GF(p))

  # Q-valued even modular symbol attached to E
  m = E.modular_symbol(1, implementation='eclib')

  # normalise the modular symbol to take integral values
    by finding the lcm of denominators
  N = lcm([m(a/p).denominator() for a in range(p)])

  # define the Manin symbol
  M = lambda a: Integer(N*m(a/p))

  # compute the rational period function
  R = 1
```

```
  for a in range(p):
    R *= (z-a)^M(a)
    if a != 0 and M(a) < 0:
      R *= (-1/a)^M(a)
  return R
```

Using this, the first line of Table 1 can be computed as below:

```
E = EllipticCurve('389A1')
p = E.conductor()
R = rational_period_function(E)
deg_R = max(R.numerator().degree(), R.denominator().degree())
num = (R-1).numerator()
factors = list(factor(num))
# list of n such that x^2 +- nx - 1 is a factor of num
yokoi = []
# list of n such that x^2 +- nx + 1 is a factor of num
mollin = []
# number of degree 1 factors of num
linear = 0
# dictionary with degrees of other factors of num
other_factors = {}
# compute yokoi, mollin, linear and other_factors
for (P, mult) in factors:
  d = P.degree()
  # if P has degree 1
  if d == 1:
    linear += mult
  # if P has the form x^2 + nx +-1
  elif d == 2 and P[0]^2 == 1:
    n = Integer(P[1])
    if P[0] == -1 and n < p/2:
      yokoi.append(n)
    if P[0] == 1 and n < p/2:
      mollin.append(n)
  else:
    # initialise the entry of other_factors corresponding to
      degree d if necessary
```

```
    if d not in other_factors.keys():
      other_factors[d] = 0
    # add the multiplicity of P to the list of factors
    other_factors[d] += mult
print(deg_R, linear, yokoi, mollin, other_factors)
```

Table 2 was obtained using a slight variation of the above code together with the following function that computes the values of any $K(z)$-valued $\mathrm{SL}_2(\mathbb{Z})$-modular symbol m (where K is a field) from its period function $R = m\{0, \infty\}$:

```
# function that returns m{r,oo} given r and the
  period function R = m{0,oo}
def mod_symb(R,r):
  # find the variable of R
  z = R.numerator().variables()[0]
  if r == 0:
      return R
  q = Integer(floor(r))
  if q != 0:
      return mod_symb(R, r-q)(z-q)
return (mod_symb(R, -1/r)/R)(-1/z)
```

(This is more or less the Euclidean algorithm.)

References

[1] A. Baker, "A remark on the class number of quadratic fields", *Bull. London Math. Soc.* **1** (1969), 98–102. MR Zbl

[2] J. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk, "Explicit Chabauty–Kim for the split Cartan modular curve of level 13", *Ann. of Math.* (2) **189**:3 (2019), 885–944. MR Zbl

[3] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk, "Quadratic Chabauty for modular curves: algorithms and examples", *Compos. Math.* **159**:6 (2023), 1111–1152. MR Zbl

[4] B. Baran, "A modular curve of level 9 and the class number one problem", *J. Number Theory* **129**:3 (2009), 715–728. MR Zbl

[5] M. Bertolini and H. Darmon, "The rationality of Stark–Heegner points over genus fields of real quadratic fields", *Ann. of Math.* (2) **170**:1 (2009), 343–370. MR Zbl

[6] A. Biró, "Chowla's conjecture", *Acta Arith.* **107**:2 (2003), 179–194. MR Zbl

[7] A. Biró, "Yokoi's conjecture", *Acta Arith.* **106**:1 (2003), 85–104. MR Zbl

[8] A. Biró and A. Granville, "Zeta functions for ideal classes in real quadratic fields, at $s = 0$", *J. Number Theory* **132**:8 (2012), 1807–1829. MR Zbl

[9] D. Byeon, M. Kim, and J. Lee, "Mollin's conjecture", *Acta Arith.* **126**:2 (2007), 99–114. MR Zbl

[10] J. W. S. Cassels, *Local fields*, London Mathematical Society Student Texts **3**, Cambridge Univ. Press, 1986. MR Zbl

[11] S. Chowla and J. Friedlander, "Class numbers and quadratic residues", *Glasgow Math. J.* **17**:1 (1976), 47–52. MR Zbl

[12] H. Cohn, *A classical invitation to algebraic numbers and class fields*, Springer, 1978. MR Zbl

[13] J. E. Cremona, "Elliptic curve data", 2001–, https://johncremona.github.io/ecdata/.

[14] H. Darmon, "Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications", *Ann. of Math.* (2) **154**:3 (2001), 589–639. MR Zbl

[15] H. Darmon and S. Dasgupta, "Elliptic units for real quadratic fields", *Ann. of Math.* (2) **163**:1 (2006), 301–346. MR Zbl

[16] H. Darmon and J. Vonk, "Singular moduli for real quadratic fields: a rigid analytic approach", *Duke Math. J.* **170**:1 (2021), 23–93. MR Zbl

[17] D. M. Goldfeld, "The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer", *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) **3**:4 (1976), 624–663. MR Zbl

[18] D. Goldfeld, "Gauss's class number problem for imaginary quadratic fields", *Bull. Amer. Math. Soc.* (*N.S.*) **13**:1 (1985), 23–37. MR Zbl

[19] R. Greenberg and G. Stevens, "p-adic L-functions and p-adic periods of modular forms", *Invent. Math.* **111**:2 (1993), 407–447. MR Zbl

[20] K. Heegner, "Diophantische Analysis und Modulfunktionen", *Math. Z.* **56** (1952), 227–253. MR Zbl

[21] M. A. Kenku, "A note on the integral points of a modular curve of level 7", *Mathematika* **32**:1 (1985), 45–48. MR Zbl

[22] M. Longo, K. Martin, and Y. Hu, "Rationality of Darmon points over genus fields of non-maximal orders", *Ann. Math. Qué.* **44**:1 (2020), 173–195. MR Zbl

[23] B. Mazur and J. Tate, "Refined conjectures of the "Birch and Swinnerton-Dyer type"", *Duke Math. J.* **54**:2 (1987), 711–750. MR Zbl

[24] B. Mazur, J. Tate, and J. Teitelbaum, "On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer", *Invent. Math.* **84**:1 (1986), 1–48. MR Zbl

[25] C. P. Mok, "On a theorem of Bertolini-Darmon on the rationality of Stark–Heegner points over genus fields of real quadratic fields", *Trans. Amer. Math. Soc.* **374**:2 (2021), 1391–1419. MR Zbl

[26] R. A. Mollin, "Class number one criteria for real quadratic fields, I", *Proc. Japan Acad. Ser. A Math. Sci.* **63**:4 (1987), 121–125. MR Zbl

[27] R. A. Mollin, "Necessary and sufficient conditions for the class number of a real quadratic field to be one, and a conjecture of S. Chowla", *Proc. Amer. Math. Soc.* **102**:1 (1988), 17–21. MR Zbl

[28] J. Oesterlé, "Nombres de classes des corps quadratiques imaginaires", exposé 631, 309–323 in *Séminaire Bourbaki*, 1983/1984, Astérisque **121-122**, 1985. MR Zbl

[29] R. Schoof and N. Tzanakis, "Integral points of a modular curve of level 11", *Acta Arith.* **152**:1 (2012), 39–49. MR Zbl

[30] J.-P. Serre, *Lectures on the Mordell–Weil theorem*, Aspects of Mathematics **E15**, Springer, 1989. MR Zbl

[31] E. de Shalit, "p-adic periods and modular symbols of elliptic curves of prime conductor", *Invent. Math.* **121**:2 (1995), 225–255. MR Zbl

[32] C. L. Siegel, "Zum Beweise des Starkschen Satzes", *Invent. Math.* **5** (1968), 180–191. MR Zbl

[33] H. M. Stark, "A complete determination of the complex quadratic fields of class number one", *Michigan Math. J.* **14** (1967), 1–27. MR Zbl

[34] H. M. Stark, "On the "gap" in a theorem of Heegner", *J. Number Theory* **1** (1969), 16–27. MR Zbl

[35] M. Watkins, "Class number problems for real quadratic fields with small fundamental unit", preprint, 2021.

[36] H. Yokoi, "Class number one problem for certain kind of real quadratic fields", pp. 125–137 in *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields* (Katata, 1986), Nagoya Univ., 1986. MR Zbl

Received 23 May 2024. Revised 18 Feb 2025.

ELIAS CAEIRO:

elias.caeiro@ens.psl.eu
Ecole Normale Supérieure, Paris, France

HENRI DARMON:

henri.darmon@mcgill.ca
Department of Mathematics and Statistics, McGill University, Montreal, QC, Canada

ESSENTIAL NUMBER THEORY

msp.org/ent

EDITOR-IN-CHIEF

Lillian B. Pierce — Duke University, pierce@math.duke.edu

EDITORIAL BOARD

Adebisi Agboola — UC Santa Barbara, agboola@math.ucsb.edu

Valentin Blomer — Universität Bonn, ailto:blomer@math.uni-bonn.de

Frank Calegari — University of Chicago, fcale@math.uchicago.edu

Laura DeMarco — Harvard University, demarco@math.harvard.edu

Ellen Eischen — University of Oregon, eeischen@uoregon.edu

Kirsten Eisenträger — Penn State University, kxe8@psu.edu

Amanda Folsom — Amherst College, afolsom@amherst.edu

Edray Goins — Pomona College, edray.goins@pomona.edu

Kaisa Matomäki — University of Turku, ksmato@utu.fi

Sophie Morel — ENS de Lyon, sophie.morel@ens-lyon.fr

James Newton — Oxford University, newton@maths.ox.ac.uk

Raman Parimala — Emory University, parimala.raman@emory.edu

Jonathan Pila — University of Oxford, jonathan.pila@maths.ox.ac.uk

Peter Sarnak — Princeton University/Institute for Advanced Study, sarnak@math.princeton.edu

Richard Taylor — Stanford University, rltaylor@stanford.edu

Anthony Várilly-Alvarado — Rice University, av15@rice.edu

John Voight — Dartmouth College, john.voight@dartmouth.edu

Melanie Matchett Wood — Harvard University, mmwood@math.harvard.edu

Zhiwei Yun — MIT, zyun@mit.edu

Tamar Ziegler — Hebrew University, tamar.ziegler@mail.huji.ac.il

PRODUCTION

Silvio Levy — (Scientific Editor), production@msp.org

See inside back cover or msp.org/ent for submission instructions.

Essential Number Theory (ISSN 2834-4634 electronic, 2834-4626 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ENT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

https://msp.org/

© 2025 Mathematical Sciences Publishers

ESSENTIAL NUMBER THEORY

2025 vol. 4 no. 1

Ray class groups and ray class fields for orders of number fields 1
GENE S. KOPP and JEFFREY C. LAGARIAS

The Heegner–Stark theorem and Stark–Heegner points 67
ELIAS CAEIRO and HENRI DARMON

An introduction to p-adic L-functions 101
JOAQUÍN RODRIGUES JACINTO and CHRIS WILLIAMS