THE HEEGNER–STARK THEOREM AND STARK–HEEGNER POINTS

ELIAS CAEIRO AND HENRI DARMON

Abstract. 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.

Contents

Notations

Given $D \equiv 0, 1 \pmod 4$, let $\mathcal{O}_D = \mathbb{Z}[\frac{D+\sqrt{D}}{2}]$ be the unique quadratic order of discriminant D, let $\mathrm{Cl}(D)$ denote its class group in the wide sense, and let $h(D)$ 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 $\mathcal{O}_{D_0}$.

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

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 $\mathrm{Cl}(D)$.

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.

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

$$D = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, \text{ and } -163. \tag{1}$$

It was originally conjectured in a slightly different form by Gauss in his *Disquisitiones Arithmeticae*, cf. [Go-85]. Heegner's original proof [He-52] exploits the theory of complex multiplication to show that the negative discriminants of class number one give rise to integral points on an affine “non-split Cartan" modular curve of level 24, reducing their classification to a tractable Diophantine problem. The method is now the object of an extensive literature. Stark's work [St-67], as well as [St-69] vindicating Heegner's approach, was immediately preceded by a proof by Baker [Ba-69] exploiting linear forms in logarithms. Variants involving modular curves of levels 5, 7, 9, 11, 13 and 17 have also been described in [Si-68], [Ke-85], [Ba-09], [ST-12], [BDMTV-19] and [BDMTV-23] respectively. See [Se-97, 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

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

Siegel showed that $L(1, \chi_D) \gg |D|^{-\epsilon}$ 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 [Go-76], [Go-85] 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

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

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 [Oe-85].

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 conjectured that there are exactly ten discriminants of the form $D = n^2 + 4$ with class number one, namely

$$D = 5,\ 8,\ 13,\ 20,\ 29,\ 53,\ 68,\ 125,\ 173,\ \text{ and }\ 293 \qquad \text{[Yo-86]}. \tag{5}$$

It is likewise believed that there are ten class number one discriminants

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

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

$$D = 5,\ 17,\ 37,\ 101,\ 197,\ \text{ and }\ 677 \qquad \text{[CF-76]}. \tag{7}$$

To yield non-trivial estimates 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, Biro was able to prove Yokoi's conjecture [Bi-03a] and Chowla's conjecture [Bi-03b] by a relatively elementary approach exploiting analytic estimates for zeta functions attached to ideal classes in real quadratic fields (cf.[BG-12]). Further more recent progress has been achieved in [Wa-19].

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 [Da-01] and developed further in [DD-04] and [DV-21], 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 and Chowla evoked above.

To briefly summarise the approach, the theory of "rigid analytic elliptic cocycles" is used to attach to any elliptic curve E of prime conductor p 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

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

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 $h(D) = 1$. A conjectural Gross-Zagier formula for Stark–Heegner points further predicts the triviality of this quadratic point if E has analytic rank ≥ 2 over $\mathbb{Q}$; it follows in this case that

$$\Phi_E(\varepsilon_D) = 1 \quad \text{whenever} \quad h(n^2+4) = 1.$$

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 prove Yokoi's conjecture, 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 $R_E(z)$. 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 $R_E(z)$ is available in terms of the *Manin symbols* for E, and the factorisation of $R_E(z) - 1$ over $\mathbb{F}_p$ is readily carried out by computer. For example, the smallest elliptic curve of rank two and prime conductor arises when $p = 389$, and the degree of $R_E(z)$ in this case is 144. The elliptic curve denoted $389A1$ in the tables of Cremona almost suffices to establish Yokoi's conjecture: it 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 classification readily follows from genus theory.

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 non-constant p-adic analytic function on a curve that vanishes at all of its rational points. One gets a full determination of the set of rational 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 entirely mysterious. See [Ca-86, Chapter 4, §6 and Chapter 10, §10] for a nice overview of Skolem's p-adic method, and [BDMTV-19] and [BDMTV-23] 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 [Da-01] 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 nothing 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—based on a highly conjectural theory—of theorems that are 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 is essentially due to Biró [Bi-03a], although it is stated in a slightly generalised form for later use in Section 7. It is the real quadratic analogue of the classical fact that every prime strictly smaller than $\frac{|D|}{4}$ is inert in K_D when D is a negative discriminant of class number one.

Proposition 1 ([Bi-03a, Fact B]). *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 $p < \frac{\sqrt{D}-2}{v}$ 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 $\frac{\sqrt{D}-1}{v}$.

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

To prove Proposition 1, we shall use the following lemma, again due to Biró.

Lemma 4 ([Bi-03a, Lemma 2]). *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*

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

then α is associated to a rational integer.

Proof. Set $\varepsilon = \varepsilon_D = u + v\frac{\sqrt{D}}{2}$, 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 $\sqrt{D} \leq \frac{2u+1}{v}$, it suffices to prove the claim for α of norm at most $\frac{2u-2}{v^2}$. In the same way, we obtain $D \geq \left(\frac{2u-1}{v}\right)^2$ and so

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

Set $v\alpha = a\varepsilon^{-1} + b$ for some rational integers a, b. We may assume that $\varepsilon^{-1} \leq |v\alpha| \leq 1$. If $a = 0$ then α is already rational so suppose $a > 0$. The conjugate $\overline{\alpha}$ of α satisfies

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

It follows that

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

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

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

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

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

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

Proof of Proposition 1. Suppose $p < \frac{\sqrt{D}-2}{v}$ 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

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

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 $\mathfrak{H}$. Falting's 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

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

is in the kernel of the natural map

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

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

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

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

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

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 that 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, namely

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

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 $\mathbb{Q}_p^\times \longrightarrow \mathcal{O}_{\mathfrak{H}_p}^\times$. 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 a map

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

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

The exceptional zero conjecture of Mazur, Tate and Teitelbaum proved by Greenberg and Stevens can be used to show the following p-adic counterpart of Proposition 5, in which the degree of cohomology is shifted by one:

Proposition 6. *The classes*

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

lie in the kernel of the natural map

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

In particular, 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 [Da-01] 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

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

satisfying the usual additivity properties of modular symbols:

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

as well as an invariance property under Γ:

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

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 non-split, and the order

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

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 $\mathcal{O}_\tau$ (a positive integer which is prime to p, by definition) is also called the discriminant of τ.

The stabiliser of τ in $\mathrm{GL}_2(\mathbb{Z}[1/p])$, denoted Γ_τ, is isomorphic to the group $\mathcal{O}_\tau^\times$ of units in $\mathcal{O}_\tau$, 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 a fundamental unit $\varepsilon_\tau > 1$ of $\mathcal{O}_\tau$, embedding it into $\mathbb{C}_p$, and requiring that γ_τ acts 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 $\mathcal{O}_\tau$ has norm -1.)

The value $J_E^\pm$ 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

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

directly analogous to (11), where $\mathfrak{H}_p^{\mathrm{RM}}$ denotes the set of RM points in $\mathfrak{H}_p$. The main conjecture of [Da-01] (see [Da-01, 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* narrrow ring class field*) attached to D.*

2. There is a Gross-Zagier formula of the form

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

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

Remark 8. Conjecture 7 can be supplemented with a conjectural Shimura reciprocity law [Da-01, Conjecture 5.9], which allows the trace in Part 2 to be expressed as a sum over the class group rather than over the Galois group of H_D/K_D. This makes Part 2 somewhat more independent of Part 1.

Remark 9. While Part 1 of Conjecture 7 seems inaccessible short of an essentially new idea, Part 2 might be amenable to the methods of [BD-09] and [Mo-21], 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 [De-95] of a tame refinement of the theorem of Greenberg-Stevens could eventually lead to a proof of, or at least partial theoretical evidence for, Part 2 of Conjecture 7.

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 J_E to lighten the notations.

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 Part 2 of Conjecture 7 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 non-trivial property of the class number one real quadratic orders in which p is inert:

Conjecture 10. *Let E be an elliptic curve of prime conductor p and analytic rank ≥ 2. If D is a discriminant of class number one for which $(\frac{D}{p}) = -1$, then $J_E[\frac{D+\sqrt{D}}{2}]$ maps to a torsion point in $E(K_D)$ under* (12). *In particular, $J_E[\frac{D+\sqrt{D}}{2}] = 1$ if E has trivial torsion over quadratic fields.*

Remark 11. If E is any elliptic curve over $\mathbb{Q}$, then $E(K_D)_{\rm tor} = E(\mathbb{Q})_{\rm tor}$ 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 12. 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 Conjecture 10 in terms of the weaker assumption on the analytic rank.

Although Conjecture 10 gives a non-trivial 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 an other can be expressed as a finite sum of *unimodular paths*, of the form $\{\frac{a}{b}, \frac{c}{d}\}$ with $ad - bc = \pm 1$, and these unimodular paths are all equivalent under Γ (under $\mathrm{SL}_2(\mathbb{Z})$, in fact) to $\{0, \infty\}$.

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

$$\Phi_E\left(\frac{1}{z}\right) = \Phi_E(z)^{-1}, \qquad \frac{\Phi_E(z+1)}{\Phi_E(z)} = \Phi_E\left(\frac{z+1}{z}\right), \tag{14}$$

as well as some 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 $\mathrm{SL}_2(\mathbb{Z})$-translates of τ arising from its continued fraction expansion (viewed as a real number)

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

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

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

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

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

The sequence $(\tau_0, \tau_1, \ldots, \tau_{m-1})$ 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 13. *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 $S = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. 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 positive coefficients and the Euclidean algrithm shows that it can be written as $T^{b_0} S T^{b_1} S \cdots T^{b_{m-1}} S$ for some positive integers $b_0, \ldots, b_{m-1} \geq 1$. The equality $\gamma_\tau \tau = \tau$ then translates to $[\overline{b_0, \ldots, b_{m-1}}]$ 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,

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

□

It transpires from Lemma 13 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 meromorphic period function Φ_E at

$$\varepsilon_D := \frac{n+\sqrt{n^2+4}}{2} = n + \cfrac{1}{n + \cfrac{1}{n + \cdots}}. \tag{15}$$

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

$$\varepsilon_D = \frac{n+\sqrt{n^2-4}}{2}$$

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

Proposition 14. *For all D of the form $n^2 \pm 4$,*

$$J_E\left[\frac{D+\sqrt{D}}{2}\right] = \Phi_E(\varepsilon_D).$$

If $D = 5$, then furthermore

$$J_E\left[\frac{1+\sqrt{5}}{2}\right] = \Phi_E(\varepsilon_5), \text{ and } J_E\left[\frac{1+\sqrt{5}}{2}\right]^2 = \Phi_E(\varepsilon_5^2).$$

Proof. For $D = n^2+4$, this follows from Lemma 13 combined with (15). In general, one can directly see that the fundamental automorph of ε_D is

$$\gamma_D = \begin{pmatrix} n & \pm 1 \\ 1 & 0 \end{pmatrix}$$

so that

$$J_E\left[\frac{D+\sqrt{D}}{2}\right] = J_E[\varepsilon_D] = J_E\{0,\gamma_D 0\}(\varepsilon_D) = J_E\{0,\infty\}(\varepsilon_D) = \Phi_E(\varepsilon_D).$$

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, $\frac{3+\sqrt{3^2-4}}{2} = \varepsilon_5^2$ is actually the square of the fundamental unit $\varepsilon_5 = \frac{1+\sqrt{5}}{2}$. 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

$$\Phi_E(\varepsilon_5^2) = J_E\left[\frac{1+\sqrt{5}}{2}\right]^2.$$

□

Proposition 14 leads to the following concrete consequence of Conjecture 10:

Conjecture 15. *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 a discriminant 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 Conjecture 15 can be proven independently of Conjecture 10.

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 and 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 $\varepsilon_{-3}=\frac{1+i\sqrt{3}}{2}$, which correspond to $\varepsilon = \frac{n+\sqrt{n^2-4}}{2}$ for $n=0,1$, we find, as in Proposition 14,

$$\gamma_{-4} = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, \qquad J_E[\varepsilon_{-4}] = \Phi_E(\varepsilon_{-4}),$$
$$\gamma_{-3} = \begin{pmatrix}1 & -1\\ 1 & 0\end{pmatrix}, \qquad J_E[\varepsilon_{-3}] = \Phi_E(\varepsilon_{-3}).$$

Lemma 16. *If $\left(\frac{-4}{p}\right)=-1$, then $J_E[\varepsilon_{-4}]=\pm 1$, and if $\left(\frac{-3}{p}\right)=-1$, 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,

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

□

Remark 17. 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, Part 2 of Conjecture 7 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. Conjecture (15) 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 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 $\mathrm{ord}_p(q) = 1$, the function $\Phi_E \in \mathcal{O}_{\mathfrak{H}_p}^{\times}/q^{\mathbb{Z}}$ can be translated by a suitable power of q to that it maps the standard affinoid $\mathfrak{H}_p^{\circ}$ to $\mathcal{O}_{\mathbb{C}_p}^{\times} \subset \mathcal{O}_{\mathbb{C}_p}$. This representative belongs to the integral Tate algebra $\mathcal{O}_{\mathfrak{H}_p^{\circ}}^{\mathrm{int}} \subset \mathcal{O}_{\mathfrak{H}_p^{\circ}}$. Reduction modulo p gives rise to maps

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

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 18. *Let $z_0 \in X(\overline{\mathbb{F}}_p)$ be a solution of the equation $R_E(z_0) = 1$, for which $R_E'(z_0) \neq 0$. Then there is a unique $z \in \mathfrak{H}_p^{\circ}$ satisfying*

$$\mathrm{red}_p(z) = z_0, \qquad \Phi_E(z) = 1.$$

We obtain the following corollary:

Corollary 19. *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 19 reduces the study of Yokoi's conjecture to the determination of the zeroes of a single rational function over $\mathbb{F}_p$, the function $R_E(z) - 1$. We now proceed to give an explicit formula for $R_E(z)$ 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*

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

defined by

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

The value $M_E(0)$ is a non-zero 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 20. *For all $r, s \in \mathbb{P}_1(\mathbb{Q})$,*

$$\bar{J}_E\{r, s\} = \prod_{a \in \mathbb{F}_p} (z - a)^{M_{rs}(a)} \pmod{\mathbb{F}_p^\times}, \tag{16}$$

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 $f : \mathbb{P}_1(\mathbb{Q}_p) \to \mathbb{C}_p^\times$,

$$⨰_{\mathbb{P}_1(\mathbb{Q}_p)} f(t)d\mu(t) := \lim_{\mathbb{P}_1(\mathbb{Q}_p) = \{U_\alpha\}} \prod_\alpha f(t_\alpha)^{\mu(U_\alpha)}$$

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 [Da-01, §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

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

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 $r, s \in \mathbb{P}_1(\mathbb{Q})$,

$$\times\!\!\!\!\!\!\int_{\tau_0}^{\tau} \int_r^s \omega_E := \times\!\!\!\!\!\!\int_{\mathbb{P}_1(\mathbb{Q}_p)} \left(\frac{\tau - t}{\tau_0 - t}\right) d\mu_E\{r, s\}(t). \tag{17}$$

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

$$J_E\{r, s\}(\tau) = \times\!\!\!\!\!\!\int^{\tau} \int_r^s \omega_E,$$

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

$$\times\!\!\!\!\!\!\int^{\tau} \int_r^s \omega_E \div \times\!\!\!\!\!\!\int^{\tau_0} \int_r^s \omega_E = \times\!\!\!\!\!\!\int_{\tau_0}^{\tau} \int_r^s \omega_E \tag{18}$$

for all $\tau_0, \tau \in \mathfrak{H}_p^\circ$ and $r, s \in \mathbb{P}_1(\mathbb{Q}_p)$. (See [Da-01, §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

$$\gamma_a = \left(\begin{smallmatrix} p & a \\ 0 & 1 \end{smallmatrix}\right) \text{ if } a \neq \infty, \quad \gamma_a = \left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right) \text{ if } a = \infty.$$

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 (17), 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 20 follows directly since the rational function on the right of (16) has the same divisor. □

By specialising this proposition to $(r,s) = (0,\infty)$ we obtain

Corollary 21. *The rational period function $R_E(z)$ satisfies*

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

Corollary 21 already suffices to compute the rational period function $R_E(z)$ 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 $R_E(z)$ in all cases.

Proposition 22. *The rational period function $R_E(z)$ is given by*

$$R_E(z) = z^{M_E(0)} \times \prod_{M_E(a)>0} (z-a)^{M_E(a)} \times \prod_{M_E(a)<0} \left(1-\frac{z}{a}\right)^{M_E(a)}, \tag{19}$$

where the products are taken over the $a \in \mathbb{F}_p^\times$. If E has (analytic) rank at least two, it is given by the simpler expression

$$R_E(z) = \prod_{a=1}^{p-1} (z-a)^{M_E(a)}. \tag{20}$$

Proof. Corollary 21 shows that (19) is true up to a multiplicative scalar. To check that this scalar is trivial, it suffices to verify that the formula for $R_E(z)$ in (19) satisfies the two and three term identities of (14) which $R_E(z)$ 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 (19) is $c^{-1}R$. After computing the first non-zero 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 $R_E(z)R_E(\frac{1}{z}) = 1$ and $R_E(\frac{z+1}{z})R_E(z) = R_E(z+1)$ amount to

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

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 $b = \frac{1}{a}$ and recalling that $M(\frac{1}{a}) = -M(a)$, and the second by grouping together a with $\frac{1}{a}$ on the right-hand-side and recalling that $M(a+1) - M(\frac{1}{a}+1) = M(a)$.

We now turn to the formula in rank ≥ 2. In this case, we need to prove that the scalar c is trivial, 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 [MT-85], 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 equal to 1 when $r \geq 2$. Evidence towards the Mazur-Tate conjecture building on the p-adic insights of Greenberg and Stevens is presented in [De-95]. 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 non-trivial refinement of the Mazur-Tate conjecture in this setting. □

6. Yokoi's conjecture

The elliptic curve of rank two and smallest prime conductor is the curve denoted $E = 389A1$ in the tables of Cremona [Cr-05], 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) $\pm 1/2$ (twice), and ± 115 (once), and twelve quadruples of roots of the form $a, -a, 1/a, -1/a$ with

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

• 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 16, by observing that the vanishing of R_E 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

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

as well as $h(-x)$, $x^{11}h(1/x)$, 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 15, there are 28 further roots given by the RM points

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

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

Repeating the same calculation with other elliptic curves of rank 2 and prime conductor, one sometimes encounters polynomials of the form $x^2 + nx \pm 1$ in the factorisation of $R_E(x) - 1$, where n is small but $D = n^2 \mp 4$ does not have class number one. These factors, while they are seemingly not accounted by Conjecture 7, are sometimes explained by a *twisted* version of the Gross-Zagier formula of Conjecture 7 [Da-01, Conjecture 5.15] (some cases of which were proven in a weaker form in [LMH-20], building on [BD-09] and [Mo-21]): if χ is a character of $\mathrm{Cl}(D) \simeq \mathrm{Gal}(H_D/K_D)$, the Néron-Tate height of the χ-isotypical component

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

of $P := J_E[\tau]$ should be a multiple of the derivative $L'(E/K_D, \chi, 1)$ of the twisted Hasse-Weil L function $L(E/K_D, \chi, s)$.

In particular, P is torsion whenever $L'(E/K_D, \chi, 1) = 0$ for every character χ of $\mathrm{Cl}(D)$. In the case where the class group is an elementary 2-group, i.e. every form is ambiguous, all the characters of $\mathrm{Cl}(D)$ are quadratic and described by genus theory as a Kronecker symbol $\left(\frac{d}{\cdot}\right)$ for some $d \mid D$. (See [Co-78, Theorem 18.27].) In this case, up to finitely many Euler factors,

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

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 $R_E - 1$ 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 non-trivial character of $\mathrm{Cl}(D_j)$ is given by $\left(\frac{5}{\cdot}\right)$. It turns out that $E^{(5)}$ has rank 2 and hence that $L'(E^{(5)}/\mathbb{Q}, 1) = 0$. It follows 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 $\Phi_E - 1$.

Our results on the factorisation of $R_E(x) - 1$ for the curve $389A1$ are summarised in the first line 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. (This curve, which also plays a key role in the work of Goldfeld-Gross-Zagier, suffices to prove Yokoi's conjecture for discriminants not divisible by 5077, but not its extension to discriminants of the form $n^2 - 4$.)

The first column 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 $R_E(z)$, 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 $R_E(z)$ above 1, which is always less than the degree of $R_E(z)$.

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 explained above. The elements 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 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 even likely to be transcendental over $\mathbb{Q}$. When such "parasitic factors" occur in the factorisation of $R_E(z)-1$, they present a more serious obstruction to proving Yokoi's conjecture or its analogue for discriminants of the form n^2-4.

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

E	$\deg(R_E)$	Linear factors	$x^2 \pm nx - 1$	$x^2 \pm nx + 1$	Degrees of other factors
$389A1$	144	68	$2, 5, 7$	$1, 4, 5, 6, 21$	11^4
$433A1$	162	62	$1, 4, 5, 11, 13$	$3, 5, 7, 9$	$5^4 10^2 12^2$
$563A1$	152	66	$1, 2, 4, 5, 7, 11$ $13, 17, \mathbf{31}, \mathbf{41}$	$0, 1, 3, 6, 7$	$2^2 6^4$
$571B1$	204	86	$2, 7, 8$	$0, 4, 6, 9, 21, \mathbf{31}$	$2^2 6^2 7^4 10^4$
$643A1$	180	58	$1, 2, 3, 4, 8, 11$	$0, 3, 4, 5, 6, 7, 9$ $11, 21, \mathbf{33}, 160^?$	$4^6 16^2$
$709A1$	296	72	$2, 3, 7, 8, 13, \mathbf{16}$	$6, 11, 21, \mathbf{24}$	$10^4 22^2 24^2 26^2$
$997B1$	460	56	$1, 2, 4, 5, 8$ $11, 17, 64^?$	$3, 5, 6, 7$	$2^6 4^2 168^2$
$997C1$	328	72	$1, 2, 4, 5, 8$ $11, \mathbf{16}, 17, \mathbf{31}$ $\mathbf{53}, 380^?, 463^?$	$3, 5, 6, 7, \mathbf{17}$	$2^6 8^4 72^2$
$5077A1$	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 $R_E - 1$

The data gathered in Table 1 is amply sufficient to prove Yokoi's conjecture. The two rows attached to the elliptic curves $389A1$ and $433A1$ imply that any class number one discriminant of the form n^2+4 with $n \geq 435$ must be divisible by both 389 and 433. But this is impossible by genus theory.

Remark 23. It may appear somewhat surprising that the fiber $R_E^{-1}(1)$ has so many $\mathbb{F}_p$-rational elements while R_E 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 less 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 $R_E - 1$ with respective multiplicites 2, 3, 2, 1, 1, 1 and 1. These also seem to be the only critical points of $R_E - 1$, i.e. roots with multiplicity ≥ 2.

For elliptic curves of rank 1, the pattern breaks down and $R_E - 1$ 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, $R_E - 1$ 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

We now turn to the determination of all the discriminants of the form $D = 4n^2 + 1$ such that $h(D) = 1$. We follow the same steps as before. 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 $\varepsilon_D = u + v\frac{\sqrt{D}}{2}$ its fundamental unit. The stabiliser of a primitive binary form $Q = ax^2 + bxy + cy^2$ of discriminant D is generated by

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

In particular, $\gamma_Q\infty$ has denominator av. Let ρ be the matrix $\left(\begin{smallmatrix} 1 & w \\ 0 & av \end{smallmatrix}\right)$ where $w = u - \frac{bv}{2}$. If τ_Q denotes a root of $Q(x,1)$, the fundamental automorph of τ_Q is $\gamma_Q^{\pm 1}$ 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 $J_E\left\{\frac{r}{v}, \infty\right\}^{\pm 1}$ for some integer $0 \leq r < v$.

Proposition 24. *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* $0 \leq r < av$ *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 $r \equiv u - \frac{bv}{2} \pmod{av}$ is coprime to av, which follows from the equality

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

□

In the previous section, we implemented this strategy when the conductor is 1, which corresponded to discriminants of the form $n^2 \pm 4$. We now proceed to do it when the conductor is 2, this time corresponding to the families $D = 4n^2 + 1$ and $D = 4(n^2 - n)$. Indeed, in the former case one has $(2n)^2 - D \cdot 1^2 = -1$ and in the latter case $(2n-1)^2 - D \cdot 1^2 = 1$.

Just like 5 both had the form $n^2 + 4$ and $n^2 - 4$, the unit $m + \sqrt{D}$, where $m \in \{2n - 1, 2n\}$ depending on the form of 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

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

be a root of $x^2 + (2n + 1)x + n$ in the former case and $x^2 + 2nx + n$ in the latter. Making Proposition 24 explicit for those families, we obtain

Corollary 25. *Let* $D > 0$ *have the form* $4n^2 + 1$ *or* $4(n^2 - n)$ *and let* $\tau_D = \frac{D+\sqrt{D}}{2}$*. Then a power of* $J_E[\tau_D]$ *is equal to* $J_E \left\{ -\frac{1}{2}, \infty \right\} (\alpha_D)$*.*

Corollary 25 and Conjecture 10 invite us to examine the quadratic factors in the factorisation of $R_E^{(2)} - 1$, where

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

As before, let E be the unique elliptic curve of rank 2 and conductor $p = 389$, labelled $389A1$ in Cremona's tables. The quadratic factors of $R_E^{(2)}$ are then

$$\begin{array}{ccccc} 2x^2 - 1 & 2x^2 - 2x - 1 & x^2 + 7x + 3 & x^2 + 11x + 5 & x^2 + 15x + 7 \\ x^2 + 27x + 13 & x^2 + 59x + 29 & x^2 + 4x + 2 & x^2 + 8x + 4 & x^2 + 20x + 10 \end{array}$$

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 24: the first two factors correspond 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 have class number two.

In the first case, the discriminant is $D = 4 \cdot 29^2 + 1 = 5 \cdot 673$ and, letting χ be the non-trivial character of $\mathrm{Cl}(D)$, one computes that the twisted Hasse-Weil L-function $L(E/K_D, \chi, s) = L(E^{(5)}/K_D, \chi, s)$ vanishes to order 3 at $s = 1$. As explained before, this is enough to suggest that the Stark-Heegner point of discriminant D is trivial.

In the second case, $D = 2^3 \cdot 3^2 \cdot 4 = 360$ and $\mathcal{O}_D$ is the order of conductor 3 in the maximal order $\mathbb{Z}[\sqrt{10}]$ of discriminant 40. Letting χ be the non-trivial character of $\mathrm{Cl}(360) = \mathrm{Cl}(40)$, the χ-component, denoted $P_{40}(\chi) \in E(H_{40})$, of the Stark-Heegner point of discriminant 40 appears to be non-trivial, since 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, general norm compatibility properties of Stark-Heegner points show 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 $P_{40}(\chi)$ need not be trivial. 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 our experiment.

Proposition 1 combined with the first line of Table 2 implies Chowla's conjecture for discriminants of conductor not divisible by 389. To deduce the full conjecture, we repeat the argument with another rank two curve of prime conductor $q \equiv 1 \pmod 4$ (for instance, $q = 433$) and invoke genus theory as in the proof of Yokoi's conjecture. As a byproduct of this analysis, we also deduce the following list of class number one discriminants of the form $4(n^2 - n)$:

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

$$D = 8, 24, 48, \textit{ and } 80.$$

Table 2 summarises the factorisation of $R_E^{(2)} - 1$ for rank 2 curves of prime conductor ≤ 1000, with the same conventions as in the previous section. For each of the two quadratic factors columns, we only write one representative for the orbit of a factor under $\left(\begin{smallmatrix}-1 & -1\\ 0 & 1\end{smallmatrix}\right)$. Note that the factor $2x^2 + 2x + 1$ that appears sometimes corresponds to the negative class number one discriminant $D = -4$ and is again explained by Lemma 16.

The integer denoted $37^?$ in the row attached to the elliptic curve $E = 571B1$ corresponds to the prime discriminant $D = 4 \cdot 37^2 + 1 = 5477$ of class number three. It would

E	$\deg(R_E^{(2)})$	Linear factors	$x^2+(2n+1)x+n$	$x^2+2nx+n$	Degrees of other factors
$389A1$	166	38	$\frac{1}{2},3,5,7,13,\mathbf{29}$	$\frac{3}{2},2,4,\mathbf{10}$	44^2
$433A1$	194	46	$1,5,13$	$5,\mathbf{10}$	$2^2 18^2 44^2$
$563A1$	176	50	$\frac{1}{2},1,3,13$	$\frac{1}{2},2,3,5,\mathbf{7}$	$4^2 42^2$
$571B1$	208	50	$\frac{1}{2},2,5,7,\mathbf{23},\mathbf{29},37^?$	$\frac{1}{2},\frac{3}{2},2,4$ $\mathbf{10},\mathbf{12}$	$4^2 25^4$
$643A1$	188	42	$\frac{1}{2},1,2,3,7,11$	$\frac{1}{2},\frac{3}{2},2,4$ $5,\mathbf{11},\mathbf{17}$	$6^4 36^2$
$709A1$	338	54	$\frac{1}{2},2,3,5,7,13$	$2,3,\mathbf{\frac{13}{2}}$	$2^4 3^4 4^4 10^2 94^2$
$997B1$	494	34	$\frac{1}{2},1,2,3,7,13$	$2,3,5$	$4^2 12^2 17^4 22^2$ $26^2 32^2 82^2$
$997C1$	354	42	$\frac{1}{2},1,2,3,7,\mathbf{11},13$	$2,3,5$	68^4
$5077A1$	4852	32	$\frac{1}{2},1,2,3,5,7,13$	$2,3,5,\mathbf{9}$	$2^2 26^2 32^2 67^4$ $75^4 101^4 110^2$ $151^4 178^4 336^2$ $346^2 394^2$

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

be interesting to check that the Hasse-Weil L-series of E twisted by any cubic unramified character of K_D vanishes to order ≥ 3, but we have not attempted this.

REFERENCES

[Ba-69] Alan Baker. *A remark on the class number of quadratic fields.* Bull. of the London Math.Soc. **1** (1969) 98–102. ↑2.

[Ba-09] Burcu Baran. *A modular curve of level* 9 *and the class number one problem.* Journal of Number Theory **129** (2009) 715–728. ↑2.

[BD-09] Massimo Bertolini and Henri Darmon. *The rationality of Stark-Heegner points over genus fields of real quadratic fields.* Ann. of Math. **170** no. 1, (2009) 343–369. ↑11, 21.

[BDMTV-19] Jennifer Balakrishnan, Netan Dogra, Steffen Müller, Jan Tuitman, and Jan Vonk. *Explicit Chabauty-Kim for the split Cartan modular curve of level* 13. Annals of Mathematics, **189** (2019) 885–944. ↑2, 5.

[BDMTV-23] Jennifer Balakrishnan, Netan Dogra, Steffen Müller, Jan Tuitman, and Jan Vonk. *Quadratic Chabauty for modular curves: algorithms and examples.* Compositio Math. **159** (2023) 1111-1152. ↑2, 5.

[BG-12] András Biró and Andrew Granville. *Zeta functions for ideal classes in real quadratic fields at $s=0$*, J. Number Theory **132** (2012) 1807–1829. ↑3.

[Bi-03a] András Biró. *Yokoi's conjecture.* Acta Arithmetica **106** (2003) 85–104. ↑3, 6.

[Bi-03b] András Biró. *Chowla's conjecture.* Acta Arithmetica **107** (2003) 179–194. ↑3.

[Ca-86] J.W.S. Cassels. *Local Fields.* Cambridge University Press (1986). ↑5.

[CF-76] S. Chowla and John Friedlander. *Class numbers and quadratic residues.* Glasgow Math. J. **17** (1976) 47–52. ↑3.

[Co-78] Harvey Cohn. *A Classical Invitation to Algebraic Numbers and Class Fields.* Springer-Verlag (1978) Universitext. ↑22.

[Cr-05] J.E. Cremona. *Tables of Elliptic Curves.* `https://johncremona.github.io/ecdata/`. ↑20.

[Da-01] Henri Darmon. *Integration on $\mathfrak{H}_p \times \mathfrak{H}$ and arithmetic applications.* Ann. of Math. (2) **154**, no. 3 (2001) 589–639. ↑3, 5, 9, 11, 18, 21.

[DD-04] Henri Darmon and Samit Dasgupta. *Elliptic units for real quadratic fields.* Annals of Math. (2) **163** (2006) 301–346. ↑3.

[De-95] Ehud de Shalit. *p-adic periods and modular symbols of elliptic curves with prime conductor.* Invent. Math. **121** (1995) 225–255. ↑11, 20.

[DV-21] Henri Darmon and Jan Vonk. *Singular moduli for real quadratic fields: a rigid analytic approach.* Duke Math J. **170** (2021) 23–93. ↑3.

[Go-76] Dorian Goldfeld. *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer.* Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **3** (1976) 624–663. ↑2.

[Go-85] Dorian Goldfeld. *Gauss's class number problem for imaginary quadratic fields.* Bull. AMS (NS) **13** (1985) 23–37. ↑2.

[He-52] Kurt Heegner. *Diophantische Analysis und Modulfunktionen.* Math Z. **56** (1952) 227–253. ↑2.

[Ke-85] M.A. Kenku. *A note on the integral points of a modular curve of level* 7. Mathematika **32** (1985) 45–48. ↑2.

[LMH-20] Matteo Longo, Kimball Martin and Yan Hu. *Rationality of Darmon points over genus fields of non-maximal orders.* Ann. Math. Québec **44** (2020) 173–195. ↑21.

[Mo-21] Chung Pang 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** (2021) 1391–1419. ↑11, 21.

[MT-85] Barry Mazur and John Tate. *Refined conjectures of the "Birch and Swinnerton-Dyer type".* Duke Math. J. **54** (1987), no. 2, 711–750. ↑20.

[Oe-85] Joseph Oesterlé. *Nombres de classes des corps quadratiques imaginaires.* Astérisque **121-122** (1985) Sém. Bourbaki exp 631, 309–323. ↑3.

[Se-97] Jean-Pierre Serre. Lectures on the Mordell-Weil theorem. *Aspects of mathematics*, Springer-Verlag (1997). ↑2.

[Si-68] C.L. Siegel. *Beweise des Starkschen Satzes.* Inventiones Math. **5** (1968) 180–191. ↑2.

[St-67] Harold M. Stark. *A complete determination of the complex quadratic fields of class number one.* Michigan Math Journal **14** (1967) 1–27. ↑2.

[St-69] Harold M. Stark. *On the "gap" in a theorem of Heegner.* J. Number Theory, **1** (1969) 16–27. ↑2.

[ST-12] René Schoof and Nikos Tzanakis. *Integral points on a modular curve of level* 11. Acta Arithmetica **152** (2012) 39–49. ↑2.

[Wa-19] Mark Watkins. *Class number problems for real quadratic fields with small fundamental unit.* Preprint (2021). ↑3.

[Yo-86] Hideo Yokoi. *Class-number one problem for certain kind of real quadratic fields.* Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986), 125–137. ↑3.

Ecole Normale Supérieure

Email address: `elias.caeiro@ens.psl.eu`

McGill University, Department of Mathematics and Statistics, Montreal, Canada

Email address: `henri.darmon@mcgill.ca`