Contemporary Mathematics

Modular algorithms for Gross–Stark units and Stark–Heegner points

Håvard Damm-Johnsen

Abstract. In recent work, Darmon, Pozzi and Vonk explicitly construct a modular form whose spectral coefficients are p-adic logarithms of Gross–Stark units and Stark–Heegner points. Here we describe how this construction gives rise to a practical algorithm for explicitly computing these logarithms to specified precision, and how to recover the exact values of the Gross–Stark units and Stark–Heegner points from them.

Key tools are overconvergent modular forms, reduction theory of quadratic forms and Newton polygons. As an application, we tabulate Gross–Stark units in narrow Hilbert class fields of real quadratic fields with discriminants up to 10000, for primes less than 20, as well as Stark–Heegner points on elliptic curves.

Contents

1. Introduction 1
2. The modular algorithm 4
3. From logarithms to invariants 11
References 22

1. Introduction

The classical theory of complex multiplication, developed by Kronecker, Weber, Fueter, Deuring, Shimura and others, gives an explicit description of abelian extensions of imaginary quadratic fields K. They are generated by *elliptic units*, which are canonical units in class fields of K. In [**Sta80**], Stark proved that logarithms of elliptic units appear as the value of derivatives of Hecke L-functions at $s = 0$, and conjectured the existence of units over arbitrary base fields, so-called *Stark units*. Heegner and Birch used CM theory to construct points on modular curves, called *Heegner points*, also defined over class fields of K. By determining the heights of their images on elliptic curves, Gross and Zagier [**GZ86**] made an important contribution towards the Birch–Swinnerton-Dyer conjecture.

2020 *Mathematics Subject Classification.* Primary 11F33, 11R42, 11Y40.

The author is supported by a scholarship from the Aker Scholarship foundation.

Let F be a real quadratic field and p a rational prime. While there is no direct analogue of the construction of elliptic units over F, Gross [**Gro81**] constructed what are now known as *Gross–Stark units*, formal powers of p-units in class fields of F, and formulated a p-adic analogue of Stark's conjectures for these. His conjecture related the value of derivatives of p-adic L-functions at $s = 0$ to local norms of Gross–Stark units, which was proved in [**DDP11**]. This was refined to a statement with norms removed in [**DKV18**], and recently Dasgupta and Kakde proved an integral version where formal units are replaced with proper units [**DK23**].

The computation of Gross–Stark units over real quadratic fields was studied in [**TY13**] when p splits in F, and [**FL22**] for p inert in F. In the real-analytic setting, in [**CR00**] Cohen and Roblot used Stark's conjectures to compute wide Hilbert class fields of real quadratic fields, and similar algorithms form the basis for general algorithms to compute ray class fields in `pari/GP`.

By analogy with Heegner points, Darmon's work [**Dar01**] uses p-adic analysis to construct points on elliptic curves. These so-called *Stark–Heegner points* are conjectured to be defined over ring class fields of F. While this conjecture is still wide open in general, it is supported by extensive computational evidence. Efficient algorithms for computing Stark–Heegner points were first introduced in [**DG02**] and [**DP06**]. Since then, the literature on algorithmic aspects of Stark–Heegner points has expanded rapidly, a selection of which is [**Gre09, GM13, GM14, GMS15, GM15**].

In [**DV21**], Darmon and Vonk introduce rigid meromorphic cocycles which take the p-adic theory beyond Stark's conjectures. Their framework gives an analogue of singular moduli for real quadratic fields, for which the techniques in this paper are expected to generalise. As a by-product, they recover a common framework for Stark units and Stark–Heegner points: in subsequent work, Darmon, Pozzi and Vonk [**DPV23**] use p-adic families of Hilbert modular forms to give an explicitly computable modular form whose spectral expansion encodes both Gross–Stark units and Stark–Heegner points.

More specifically, the authors construct a classical modular form G from a parallel weight 1 Hilbert Eisenstein series $E_{1,1}$ over a real quadratic field F in which p is inert. First, they define the *anti-parallel weight deformation* of $E_{1,1}$, and modify by a linear combination of Eisenstein families. Then they restrict the argument to the diagonally embedded upper half plane $\mathfrak{h}$ in $\mathfrak{h} \times \mathfrak{h}$, and differentiate with respect to the weight. This is shown to be a p-adic modular form, to which they finally apply Hida's ordinary projector to get the modular form $G \in M_2(\Gamma_0(p))$. They also prove that the form is non-trivial when F has no unit of negative norm.

A straightforward consequence of the theorems in [**DPV23**] is the following:

Theorem 1.1. *Suppose F has no unit of negative norm. Then*

$$\langle G, f\rangle_{\Gamma_0(p)} = \begin{cases} \frac{1}{p-1}\log_p u & \textit{if } f = E_2^{(p)}, \\ L_{\mathrm{alg}}(1,f)\log_{E_f} P_f & \textit{if } f \textit{ is a cuspidal eigenform with coefficients in } \mathbb{Q}. \end{cases}$$

Here u is a Gross–Stark unit, $E_2^{(p)}$ the Eisenstein series on $M_2(\Gamma_0(p))$, and $L_{\mathrm{alg}}(1,f)$ the algebraic part of the special value $L(1,f)$ of the L-function attached to f. E_f is the elliptic curve associated to f via the Eichler–Shimura construction, $\log_{E_f}$ the formal logarithm on E_f, and P_f a Stark–Heegner point on E_f, conjecturally defined over the narrow Hilbert class field of F. A more precise statement may be found in Theorem 2.2.

29 Jun 2023 06:07:20 PDT
230121-Damm Version 2 - Submitted to LuCaNT

The goal of this paper is to show that the steps defining G can be made completely explicit in a computer algebra system such as `sage` [**The22**] or `magma` [**BCP97**], and in particular we can compute the spectral coefficients of G to arbitrary precision. A key tool is algorithms for overconvergent modular forms due to Lauder [**Lau11, Lau14**], with necessary modifications for $p \in \{2,3\}$ from [**Von15**]. As a proof of concept, we compute tables of Gross–Stark units over $\mathbb{Q}(\sqrt{D})$ for fundamental discriminants $D < 10000$ and $p < 20$, and Stark–Heegner points on elliptic curves for $D < 100$, $p < 20$. This can be viewed as a numerical verification of the aforementioned conjecture stated in [**DV22**]. For p equal to 2 or 3, these tables are virtually complete, with only a handful of omissions due to the large height of the polynomials.

Example 1.2. Let $D = 8441 = 23 \cdot 367$. Then $F \coloneqq \mathbb{Q}(\sqrt{D})$ has narrow class number 26, and combining Algorithm 2 and Algorithm 5 gives the polynomial

$$\begin{aligned}
3^{43}x^{26} - 3^{28}\cdot 74700593x^{25} & + 3^{21}\cdot 413213377697x^{24} \\
-3^{14}\cdot 1491793680346193x^{23} & + 3^{11}\cdot 48103058975883121x^{22} \\
-3^{8}\cdot 1176950719953501830x^{21} & + 3^{8}\cdot 841442767734656470x^{20} \\
-3^{6}\cdot 5230173358710191479x^{19} & + 3^{7}\cdot 1983729129037937219x^{18} \\
-3^{5}\cdot 28800297384178354201x^{17} & + 3^{6}\cdot 13798304822142405250x^{16} \\
-3^{2}\cdot 131401208998818663362 5x^{15} & + 3^{2}\cdot 135008529703506577835 6x^{14} \\
-1207461049666092903072 5x^{13} & + 3^{2}\cdot 135008529703506577835 6x^{12} \\
-3^{2}\cdot 131401208998818663362 5x^{11} & + 3^{6}\cdot 13798304822142405250x^{10} \\
-3^{5}\cdot 28800297384178354201x^{9} & + 3^{7}\cdot 1983729129037937219x^{8} \\
-3^{6}\cdot 5230173358710191479x^{7} & + 3^{8}\cdot 841442767734656470x^{6} \\
-3^{8}\cdot 1176950719953501830x^{5} & + 3^{11}\cdot 48103058975883121x^{4} \\
-3^{14}\cdot 1491793680346193x^{3} & + 3^{21}\cdot 413213377697x^{2} \\
-3^{28}\cdot 74700593x & + 3^{43}.
\end{aligned} \tag{1.1}$$

The roots of this polynomial are 3-units generating the narrow Hilbert class field of F, a degree 52 extension of $\mathbb{Q}$, and their square roots are Gross–Stark units attached to narrow ideal classes in F, as defined in Section 3.

Example 1.3. Let $p = 11$ and consider $E : y^2 + y = x^3 - x^2 - 10x - 20$, a model for $X_0(11)$. Using Algorithm 6 we find the points on E described in Table 1. For each

TABLE 1. Table of Stark–Heegner points on $E : y^2+y = x^3 - x^2 - 10x - 20$, for $D < 100$.

D	X	Y	P
21	x^2+3x+4	x^2+3x+4	$11x^2-6x+11$
24	x^2+8	$x^2+10x+57$	$11x^2-14x+11$
28	$x^2+\frac{71}{16}x+\frac{23}{4}$	$x^2-\frac{101}{64}x+\frac{599}{64}$	$11x^2-6x+11$
57	$x+\frac{1065}{304}$	$x^2+x+\frac{1130412905}{28094464}$	$11x^2-3x+11$
76	$x+\frac{1065}{304}$	$x^2+x+\frac{1130412905}{28094464}$	$11x^2-3x+11$

row, the polynomials in columns X and Y are the minimal polynomials of the x- and

29 Jun 2023 06:07:20 PDT
230121-Damm Version 2 - Submitted to LuCaNT

y-coordinates, respectively, of a Stark–Heegner point on E defined over the narrow Hilbert class field of $\mathbb{Q}(\sqrt{D})$. This field is generated over $\mathbb{Q}(\sqrt{D})$ by a root of the polynomial P in the final column. For example, for $D = 24$, $(2\sqrt{-2}, 5 + 4\sqrt{-2})$ is a Stark–Heegner point on $X_0(11)$ defined over $\mathbb{Q}(\sqrt{24}, \sqrt{-2})$, which is the splitting field over $\mathbb{Q}(\sqrt{24})$ of $11x^2 - 14x + 11$.

Our paper is structured as follows: in Section 2 we first give a precise definition of Gross–Stark units and describe properties of Stark–Heegner points, then discuss the results of [**DPV23**] and explain how to use the classical reduction theory of indefinite binary quadratic forms to greatly improve the efficiency of the resulting algorithms. Next, in Section 3 we use the Brumer–Stark conjecture to recover a Gross–Stark unit from its p-adic logarithm, and describe how to compute a Stark–Heegner point from its formal logarithm. We also discuss how to verify the correctness of the data computed. Finally, we present data computed and make some observations.

The algorithms in our paper are implemented in both `magma` and `sage`, and can be found in the repositories `https://github.com/havarddj/drd` and `https://github.com/havarddj/hilbert-eisenstein`.

Acknowledgements: I am very grateful to Jan Vonk for suggesting the problem and for continued guidance and suggestions, and to James Newton for helpful conversations and comments on the paper. Thanks to Alex Braat for suggesting the statement of Lemma 3.9, Samuel Frengley for help with `magma`, and to Alex Horawa and George Robinson for enlightening conversations. Finally, I am grateful to the anonymous reviewers who provided a large number of comments improving the content, language and exposition of the article.

2. The modular algorithm

2.1. Notation. For the remainder of the paper, F will denote a real quadratic extension of $\mathbb{Q}$ of discriminant D, and $\mathcal{O}_F$ its ring of integers. Its different ideal, which is principal and generated by $\sqrt{D}$, will be denoted $\mathfrak{d}$. If $\alpha \in F$, let α' be its conjugate.

We let Cl^+ be the narrow Hilbert class group of F, so that $\mathrm{Cl}^+ \cong G := \mathrm{Gal}(H/F)$ where H is the narrow Hilbert class field of F, the maximal abelian extension of F unramified at all finite places, of degree h^+. For $\sigma \in G$, the corresponding class in Cl^+ is denoted A_σ, and conversely a class A in Cl^+ determines an automorphism $\sigma_A \in G$. The narrow ideal class group is strictly larger than the wide ideal class group if and only if F has no units of norm -1, and in light of Theorem 1.1 we restrict our attention to this case. Under this assumption, the principal ideal $\mathfrak{d}$ defines an element of order 2 in Cl^+. Furthermore, H is a CM extension of the wide Hilbert class field, and the automorphism $\kappa = \sigma_{\mathfrak{d}}$ plays the role of complex conjugation in G. We frequently write $\bar{\alpha}$ instead of $\kappa(\alpha)$ if the meaning is clear from the context.

Let p be a rational prime inert in F. Then p splits completely in H, and we fix a prime $\mathfrak{P}$ of H above p. This determines an isomorphism of completions $F_p \cong H_{\mathfrak{P}}$. A function $f : \mathrm{Cl}^+ \to \mathbb{C}$ is odd if $f(A[\mathfrak{d}]) = -f(A)$ for all $A \in \mathrm{Cl}^+$. The field generated by the values of a character ψ is denoted by $\mathbb{Q}(\psi)$.

We say an element $\alpha \in F$ is totally positive if $\rho(\alpha) > 0$ for all embeddings $\rho \colon F \hookrightarrow \mathbb{R}$, and we write $\alpha \gg 0$. If $X \subset F$ is any subset, we set $X_+ := \{\alpha \in X : \alpha \gg 0\}$.

Given an integral ideal $\mathfrak{a}$ of F, let $N(\mathfrak{a}) := \#(\mathcal{O}_F/\mathfrak{a})$, and this extends to fractional ideals by $N(\mathfrak{a}/\mathfrak{b}) := N(\mathfrak{a})/N(\mathfrak{b})$, and to elements $\alpha \in F^\times$ by $N(\alpha) = N((\alpha))$, where (α) denotes the fractional ideal generated by α. By convention, we also set $N(x) = x^2$ when x is an indeterminate. For any number field K, $\mu(K)$ denotes the set of all roots of unity in K.

If $\mathfrak{P}$ is a non-zero prime ideal of H and $\alpha \in H^\times$, then we set $|\alpha|_{\mathfrak{P}} = N(\mathfrak{P})^{-\operatorname{ord}_{\mathfrak{P}} \alpha}$, where $\operatorname{ord}_{\mathfrak{P}} \alpha$ denotes the power of $\mathfrak{P}$ appearing in the prime ideal factorisation of (α). This is the so-called normalised absolute value with respect to $\mathfrak{P}$, and in particular $N(\mathfrak{P}) = p^2$ in the present setting. All of our absolute values will be normalised, and we refer to [**Gro81**, p. 980] for a general definition which applies to both the finite and infinite places of H.

The p-units in H is the group $\mathcal{O}_H[1/p]^\times := \{\alpha \in H^\times : |\alpha|_v = 1 \text{ if } v \nmid p\}$, where v runs over all places of H. In particular, $\alpha \in \mathcal{O}_H[1/p]^\times$ has absolute value 1 under every embedding $H \hookrightarrow \mathbb{C}$. This is a finitely generated abelian group by a version of Dedekind's unit theorem, [**NS13**, Cor. 11.7].

2.2. Gross-Stark units and Stark–Heegner points. Gross [**Gro81**, Prop. 3.8] proved the existence and uniqueness of a "formal power of a p-unit" $u \in \mathcal{O}_H[1/p]^\times \otimes \mathbb{Q}$ characterised by the properties

$$\operatorname{ord}_{\mathfrak{P}} \sigma(u) = \zeta(0, A_\sigma) \text{ for all } \sigma \in G \quad \text{and} \quad \bar{u} = 1/u, \tag{2.1}$$

where the bar denotes complex conjugation, and $\zeta(s, A_\sigma)$ is the partial L-function defined by the Dirichlet series $\zeta(s, A_\sigma) = \sum_{\mathfrak{a} \leq \mathcal{O}_F,\, [\mathfrak{a}] = A_\sigma} N(\mathfrak{a})^{-s}$, which admits a meromorphic continuation to $\mathbb{C}$ in the usual manner. This depends only on the choice of prime $\mathfrak{P}$ of H above p. In [**DPV23**, Eq. (4)], the authors twist by elements of G to get units $u_A := \sigma_A(\bar{u})$ indexed by $A \in \mathrm{Cl}^+$, equal to u_τ when $A = [\mathbb{Z} + \tau\mathbb{Z}]$ in their notation. It is therefore characterised by

$$\operatorname{ord}_{\mathfrak{P}^\sigma} u_A = -\zeta(0, AA_{\sigma^{-1}}) \text{ for all } \sigma \in G \quad \text{and} \quad \bar{u}_A = 1/u_A. \tag{2.2}$$

This is referred to as the *Gross–Stark unit attached to A*. Note that these are all G-conjugate: $\sigma(u_A) = u_{AA_\sigma}$.

The Brumer–Stark conjecture, proven up to powers of 2 in [**DK23**], implies that u_A^e, where $e = \#\mu(H)$, gives an element of $\mathcal{O}_H[1/p]^\times$. More precisely, there exists an element $\epsilon \in \mathcal{O}_H[1/p]^\times$ satisfying $\epsilon \otimes 1 = e \cdot u$ such that $H(\sqrt[e]{\epsilon})/F$ is an abelian extension. We set $\epsilon_A := \sigma_A(\bar{\epsilon})$, which we refer to as the *Brumer–Stark unit attached to A*. These are the units we compute in Section 3. An immediate consequence of the second part of Equation (2.2) is that ϵ_A lies on the unit circle under any embedding $H \hookrightarrow \mathbb{C}$. For the remainder of the paper, we will assume the full Brumer–Stark conjecture. Our computations can then be viewed as a verification of the conjecture.

We also attach a Gross–Stark unit to a character $\psi : G \to \mathbb{C}^\times$ by setting

$$u_\psi := \prod_{A \in \mathrm{Cl}^+} u_A^{\psi(A)} = \prod_{\sigma \in G} \sigma(\bar{u})^{\psi(A_\sigma)}, \tag{2.3}$$

which lies in $\mathcal{O}_H[1/p]^\times \otimes \mathbb{Q}(\psi)$, and satisfies $\operatorname{ord}_{\mathfrak{P}} u_\psi = -L(0, \psi)$ and $\sigma(u_\psi) = \bar{\psi}(A_\sigma) u_\psi$ for all $\sigma \in G$. This is compatible with the notation in [**DDP11**].[1]

[1] However, it is different from the formula in [**DPV23**, Eq. (51)], in which u_ψ depends on τ, and the corresponding formula for $\operatorname{ord}_{\mathfrak{P}} u_\psi$ in the proof of Lemma 3.5 is off by a factor of $\psi(\sigma_A)$, or $\psi(\tau)$ in their notation.

29 Jun 2023 06:07:20 PDT
230121-Damm Version 2 - Submitted to LuCaNT

Stark–Heegner points $P_{\psi,f}$ are defined in [**Dar01**] and [**Das05**], and for brevity we give a description of their properties instead of a strict definition. They are defined on the modular Jacobian $J_0(p)$, which is an elliptic curve when the genus of $X_0(p)$ is one. More generally, if $J_0(p)$ splits into a product of abelian varieties of which one is an elliptic curve E, then there exists a cuspidal eigenform $f \in S_2(\Gamma_0(p))$ such that E is isogenous to E_f, and $P_{\psi,f}$ gives a point on these. The reader can find further details in [**DV22**, §3.7].

Pick an elliptic curve E_f in the isogeny class. In this setting, $P_{\psi,f}$ comes from an element of F_p defined via p-adic analytic methods. By [**Sil09**, Thm. 14.1], $E_f(F_p)$ is isomorphic to $F_p^\times/q^{\mathbb{Z}}$ where q is the Tate parameter attached to E_f. We can find an explicit isomorphism $E_f(F_p) \to F_p^\times/q^{\mathbb{Z}}$ as follows: first find an isomorphism between E_f and the corresponding Tate curve E_q by computing their Weierstraß equations and using the command `IsIsomorphic` in `magma`. Then compute the isomorphism $E_q \to F_p^\times/q^{\mathbb{Z}}$ using the formulae in [**Sil09**, §C.14]. This gives a point $P_{\psi,f}$ in $E_f(F_p)$. However, it is conjectured in [**Dar01**] that it is actually defined over H via the embedding $H \hookrightarrow H_{\mathfrak{P}} \cong F_p$, and in Section 3.2 we verify this computationally.

2.3. Diagonal restriction derivatives. Let ψ be an odd character on Cl^+. Following [**DPV23**] we consider the Hilbert modular Eisenstein series $E_{1,1}(\psi)$ of parallel weight 1 whose q-expansion at the cusp $\mathfrak{d}$ is given by the series

$$E_{1,1}(\psi)_{\mathfrak{d}} = \sum_{\nu \in \mathfrak{d}_+^{-1}} \sigma_{0,\psi}(\nu\mathfrak{d}) q^{\operatorname{tr}\nu}, \tag{2.4}$$

where $\sigma_{0,\psi}(\nu\mathfrak{d})$ is the divisor sum

$$\sigma_{0,\psi}(\nu\mathfrak{d}) := \sum_{\mathfrak{a}|\nu\mathfrak{d}} \psi(\mathfrak{a}). \tag{2.5}$$

For p a rational prime inert in F, we also define the p-stabilisation of $E_{1,1}(\psi)$ by $E_{1,1}^{(p)}(\psi)(z_1,z_2) := E_{1,1}(\psi)(z_1,z_2) - pE_{1,1}(\psi)(pz_1,pz_2)$. There is a certain p-adic family of modular forms $\mathcal{F}^+$, a linear combination of two Eisenstein families along with the *anti-parallel weight deformation*, whose weight 1 specialisation equals $E_{1,1}^{(p)}(\psi)$. Note that $\mathcal{F}^+$ is different from the parallel weight Eisenstein family used in [**DPV21**], and computing its q-expansion requires a fairly delicate argument using Galois deformation theory, the details of which are in [**DPV23**, §3]. Since $E_{1,1}^{(p)}(\psi)(z,z)$ is a classical modular form of level 1 and weight 2 and therefore identically 0, $E_{1,1}^{(p)}(\psi)$ vanishes along the diagonally embedded copy of $\mathfrak{h}$ in its domain $\mathfrak{h} \times \mathfrak{h}$. Taking the derivative of $\mathcal{F}^+$ in the weight space and restricting to weight 1 then gives an overconvergent modular form in one variable, denoted by ∂f_ψ^+. We refer to this as the *diagonal restriction derivative*, and its q-expansion is given as follows:

Proposition 2.1 ([**DPV23**, Prop. 4.6])**.** *The diagonal restriction derivative is an overconvergent modular form of weight* 2 *and tame level* 1 *with q-expansion*

$$\partial f_\psi^+(q) = \frac{1}{2}\log_p(u_\psi) - \sum_{n=1}^{\infty} \sum_{\substack{\nu \in \mathfrak{d}_+^{-1} \\ \operatorname{tr}\nu = n}} \sum_{\substack{\mathfrak{a}|(\nu)\mathfrak{d} \\ (\mathfrak{a},p)=1}} \psi(\mathfrak{a}) \log_p\left(\frac{\nu\sqrt{D}}{N(\mathfrak{a})}\right) q^n. \tag{2.6}$$

29 Jun 2023 06:07:20 PDT
230121-Damm Version 2 - Submitted to LuCaNT

It has rate of overconvergence r for each $r < p/(p+1)$.

The symbol $\log_p$ denotes the p-adic logarithm, defined by the power series $\log_p(1-x) = \sum_{n=1}^{\infty} x^n/n$ on its domain of convergence in $\mathcal{O}_{F_p}$, and extended by setting $\log_p(p) = \log_p(\zeta) = 0$ for any root of unity ζ in F_p. To evaluate this at elements of F, we identify F with its image in F_p.

Applying Hida's ordinary projection operator e_{ord} to ∂f_{ψ}^{+} gives a classical modular form of level $\Gamma_0(p)$ and weight 2. The space of such forms is spanned by the Eisenstein series

$$E_2^{(p)}(z) = \frac{p-1}{24} + \sum_{n=1}^{\infty} \Big(\sum_{\substack{d \mid n \\ (d,p)=1}} d \Big) q^n, \tag{2.7}$$

along with eigenforms f, which we normalise so that $a_1(f) = 1$ in the q-expansion at ∞.

Theorem 2.2. *Set $F = \mathbb{Q}(\sqrt{D})$ and let p be a prime inert in F. Write*

$$e_{\mathrm{ord}}(\partial f_{\psi}^{+}) = \lambda_0 E_2^{(p)} + \sum_f \lambda_f f, \quad \text{where} \quad \lambda_0, \lambda_f \in F_p. \tag{2.8}$$

Then $\lambda_0 = \frac{1}{p-1} \log u_{\psi}$, and if $a_n(f) \in \mathbb{Q}$ for all n, then $\lambda_f = L_{\mathrm{alg}}(1,f) \log_{E_f}(P_{\psi,f})$, where $P_{\psi,f}$ is a Stark–Heegner point in $E_f(\mathbb{C}_p)$, the elliptic curve attached to f by the Eichler–Shimura construction, and $L_{\mathrm{alg}}(1,f)$ is the algebraic part of the value $L(1,f)$.

Conjecture 3.19 in [**DV22**] states that the points $P_{\psi,f}$ are in fact algebraic, defined over the narrow Hilbert class field of F.

Proof of Theorem 2.2. By [**DPV23**, Prop. 4.7], $G \coloneqq e_{\mathrm{ord}}(\partial f_{\psi}^{+})$ can be written as a generating series[2]

$$2G(z) = \log_p(u_{\psi}) + \sum_{n=1}^{\infty} \log_p(T_n J_w[\psi]) q^n. \tag{2.9}$$

Meanwhile, by [**DPV23**, eq. 29] the cocycle J_w decomposes as follows:

$$J_w = \frac{2}{p-1} J_{\mathrm{DR}} + 2 \sum_f L_{\mathrm{alg}}(1,f) J_f^{-} \bmod J_{\mathrm{univ}}^{\mathbb{Z}}, \tag{2.10}$$

Plugging the expression for J_w into the n-th Fourier coefficient for $n \geq 1$ coprime to p, we obtain

(2.11a)
$$a_n(G) = \frac{2}{p-1} \log_p T_n J_{\mathrm{DR}}[\psi] + 2 \sum_f L_{\mathrm{alg}}(1,f) \log_p T_n J_f^{-}[\psi]$$

$$= \frac{2}{p-1} \log_p(J_{\mathrm{DR}}[\psi]) \cdot a_n(E_2^{(p)}) + \sum_f L_{\mathrm{alg}}(1,f) \log_p(J_f^{-}[\psi]) \cdot a_n(f). \tag{2.11b}$$

Theorem B of [**DPV23**] combined with the proof of Theorem 4.8 in the same paper implies that $J_{\mathrm{DR}}[\psi] = u_{\psi}^{24}$, and conjecture 3.19 in [**DV22**] implies that $J_f^{-}[\psi]$ maps

[2] There is a sign missing in the proof of Thm. 4.8 which propagates back to Prop. 4.7. As written, the constant term of the Eisenstein series in the spectral expansion is off by a factor of -1. We assume here that the statement of Thm. 4.8 is correct as written.

to $P_{\psi,f} \in E_f(F_p)$ under the Tate uniformisation. Denoting the composite of the Tate map and $\log_p$ by $\log_{E_f}$, we get that

$$a_n(G) = \frac{24}{p-1} \log_p(u_\psi) \cdot a_n(E_2^{(p)}) + \sum_f L_{\mathrm{alg}}(1,f) \log_{E_f} P_{\psi,f} \cdot a_n(f). \tag{2.12}$$

As in the proof of [**DPV23**, Prop. 4.7], there exists a modular form in $M_2(\Gamma_0(p))$ with prime to p coefficients $a_n(G)$, which we denote by g. Now $g - G$ is an oldform in $M_2(\Gamma_0(p))$ as all its coefficients of index coprime to p vanish, hence equals 0, and this completes the proof. $\square$

This construction can be made completely explicit in a computer algebra system such as `magma` or `sage`, at least to finite p-adic precision:

(1) Compute the terms $\{a_n\}_{n=1}^M$ of the q-expansion of ∂f_ψ^+ in Equation (2.6) up to a certain bound M by enumerating the elements $\nu \in \mathfrak{d}_+^{-1}$ of trace n and factorising $\nu\mathfrak{d}$. Since $\log_p(xy) = \log_p x + \log_p y$ for any $x, y \in F_p$, we only need to evalute this once per n.
(2) Compute a basis for the space of overconvergent modular forms to sufficiently high precision using [**Lau11**, Algorithm 1].
(3) Solve for ∂f_ψ^+ and its constant term in this basis.
(4) Compute the ordinary projection as a matrix on the basis, and apply to the vector defining ∂f_ψ^+ to get $e_{\mathrm{ord}}(\partial f_\psi^+)$. This is described in detail in step (6) of [**Lau14**, Alg. 2.1].
(5) Solve for $e_{\mathrm{ord}}(\partial f_\psi^+)$ in an eigenbasis of $M_2(\Gamma_0(p))$, which can be found explicitly using built-in methods in `sage` and `magma`.

In practice, the first step is very slow due to the cost of evaluating $\psi(\mathfrak{a})$ for many $\mathfrak{a}$. Moreover, the coefficients of ∂f_ψ^+ lie in an extension of F_p generated by the values of ψ, which is of high degree if the narrow class number of F is large.

2.4. Improvements using quadratic forms. To get around these difficulties, we combine two observations: the first is that if we split the sum into a sum over classes $A \in \mathrm{Cl}^+$, then it suffices to compute sums corresponding to all pairs $(\nu, \mathfrak{a})$ where $\mathfrak{a} \mid \nu\mathfrak{d}$ and $\mathfrak{a}$ has class A in the narrow class group, which lie in F_p. The second is that by the correspondence between ideals of $\mathbb{Q}(\sqrt{D})$ and indefinite binary quadratic forms of discriminant D, we can use reduction theory to enumerate all such ideals.

Proposition 2.3 ([**Cox11**, Ex. 7.21])**.** *There is a map between ideals of $\mathbb{Q}(\sqrt{D})$ and indefinite binary quadratic forms of discriminant D, induced by the map*

$$\mathfrak{a} = \alpha\mathbb{Z} + \beta\mathbb{Z} \mapsto \frac{N(x\alpha - y\beta)}{N(\mathfrak{a})}, \tag{2.13}$$

This map respects the class group structure: two ideals are in the same narrow ideal class if and only if the corresponding quadratic forms are equivalent under the action of $\mathrm{SL}_2(\mathbb{Z})$,

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} \cdot Q = Q(rx + sy, tx + uy). \tag{2.14}$$

We say that an indefinite quadratic form $Q(x,y) = ax^2 + bxy + cy^2$ is **reduced** if $|\sqrt{D} - 2|a|| < b < \sqrt{D}$. Any given form is equivalent to at most finitely many reduced forms.

Proposition 2.4. *Let $F = \mathbb{Q}(\sqrt{D})$ be a real quadratic field and $A \in \mathrm{Cl}^+$ a fixed class with associated reduced quadratic form Q_0. Then there is a bijection between*

$$\mathbb{I}(n, A) := \left\{ (\mathfrak{a}, \nu) : \begin{array}{l} \nu \in \mathfrak{d}_+^{-1},\ \operatorname{tr}\nu = n \\ \mathfrak{a} \mid (\nu)\mathfrak{d},\ [\mathfrak{a}] = A \end{array} \right\} \tag{2.15}$$

and

$$M(n, A) := \left\{ (Q = ax^2 + bxy + cy^2, \gamma) : \begin{array}{l} \gamma \in N_n,\ Q \sim Q_0^\gamma, \\ a > 0 > c \end{array} \right\}, \tag{2.16}$$

where N_n is a set of double coset representatives of

$$\mathrm{SL}_2(\mathbb{Z}) \setminus \{\gamma \in \mathrm{Mat}_2(\mathbb{Z}) : \det\gamma = n\} / \operatorname{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(Q_0). \tag{2.17}$$

Proof. This is essentially [**LV22**, Lemma 4.1], except we identify τ with its associated quadratic form. □

We call an element $Q \in M(n, A)$ a *nearly reduced form* since although it might not be reduced in the strict sense, it is an element of the reduced cycle of Q_0, as defined in [**BV07**, Ch. 6]. Note that N_n can be found as a subset of the coset representatives of $\mathrm{SL}_2(\mathbb{Z}) \setminus \{\det\gamma = n\}$, which we can choose to be

$$\begin{pmatrix} n/m & j \\ 0 & m \end{pmatrix}, \qquad m|n,\ 0 \le j \le m-1,\ (m, n/m) = 1. \tag{2.18}$$

The sets $M(n, A)$ and $M(d, A)$ for $d \mid n$ are not independent: if $Q \sim Q_0^{\gamma_n}$ for some $\gamma_n \in N_n$, then we can find corresponding elements γ_d and $\gamma_{n/d}$ such that $\gamma_n = \gamma_d\gamma_{n/d}$, and so we can generate it in $M(n, A)$ by applying suitable Hecke matrices to pairs in $M(d, A)$. This gives a recursive algorithm for computing $M(n, A)$, described in Algorithm 1.

It is convenient to work with so-called *odd indicator functions on* Cl^+, meaning functions of the form

$$\mathbf{1}_A^*(B) := \mathbf{1}_A(B) - \mathbf{1}_{A[\sqrt{D}]}(B) = \begin{cases} 1 & \text{if } \ B = A, \\ -1 & \text{if } \ B = A[\sqrt{D}], \\ 0 & \text{otherwise.} \end{cases} \tag{2.19}$$

We can pass between odd characters and odd indicator functions via the change of basis formulae

$$\psi(A) = \frac{1}{2}\sum_{B \in \mathrm{Cl}^+} \psi(B)\mathbf{1}_B^*(A) \quad \text{and} \quad \mathbf{1}_A^*(B) = \frac{2}{h^+}\sum_{\psi \text{ odd}} \psi(B)\bar{\psi}(A). \tag{2.20}$$

These are simple consequences of the orthogonality relations for characters, see [**Ser77**, §2.3]. By linearity, we obtain the following version of Proposition 2.1:

Corollary 2.5. *Fix an indefinite quadratic form Q corresponding to a class $A \in \mathrm{Cl}^+$. The series $\partial f_Q^+(q) = \log_p(u_A) + \sum_{n=1}^\infty a_n(\partial f_Q^+)$, where*

$$a_n(\partial f_Q^+) = -\sum_{n=1}^{\infty} \left(\sum_{\substack{(Q,\gamma) \in M(n,A) \\ Q = \langle a,b,c\rangle \\ (a,p)=1}} \log_p\left(\frac{-b + n\sqrt{D}}{2a}\right) - \sum_{\substack{(Q,\gamma) \in M(n,A[\sqrt{D}]) \\ Q = \langle a,b,c\rangle \\ (a,p)=1}} \log_p\left(\frac{-b + n\sqrt{D}}{2a}\right) \right) q^n, \tag{2.21}$$

defines an r-overconvergent modular form of weight 2 and tame level 1 for any $r < p/(p+1)$.

Algorithm 1: Compute the set $M(n, A)$ of nearly reduced forms.

Input:
- A fundamental discriminant D,
- A class A in Cl^+ represented by a reduced quadratic form Q_0,
- A positive integer n.

Output: A set of sets $\{M(d, A)\}$ indexed by divisors $d \mid n$.

if $n = 1$ **then**
 return $\{\{Q, \mathbf{1}\}\}$
$M_n \leftarrow \emptyset$ `// Initialise` M_n
$p \leftarrow$ smallest prime dividing n
$d \leftarrow n/p$
$M_d \leftarrow M(d, A)$
$H_p \leftarrow \left\{ \begin{pmatrix} p/m & j \\ 0 & m \end{pmatrix} : m \in \{1, p\},\ 0 \leq j \leq m-1 \right\}$
for $(Q_d, \gamma_d) \in M_d$ **do**
 for $\delta \in H_p$ **do**
  $Q' \leftarrow Q_d^\delta$
  if $Q' \not\sim_{\mathrm{SL}_2(\mathbb{Z})} Q$ *for all* $(Q, \gamma) \in M_n$ **then**
   $Q_1, \ldots, Q_c \leftarrow$ `ReducedCycle`(Q')
   $M_n \leftarrow M_n \cup \{(Q_1, \delta\gamma_m) \ldots, (Q_c, \delta\gamma_m)\}$
return $\{M_d : d \mid n\}$

Proof. Define $\partial f_Q^+(q) := \frac{2}{h^+} \sum_{\psi \text{ odd}} \bar{\psi}(A) \partial f_\psi^+(q)$, which has the effect of replacing $\psi(\mathfrak{a})$ in Equation (2.6) with $\mathbf{1}_A^*([\mathfrak{a}])$. Being a linear combination of overconvergent modular forms, it is itself overconvergent of the same weight, level and rate of overconvergence.

Using Proposition 2.4, we can rewrite the series in terms of $M(n, A)$ and $M(n, A[\sqrt{D}])$, showing that Equation (2.21) holds for the non-constant terms. To compute the constant term of $\partial f_Q^+(q)$, note that formally, $u_\psi = \sum_{A \in \mathrm{Cl}^+} \psi(A) \cdot u_A$, so

$$\frac{2}{h^+} \sum_{\psi \text{ odd}} \bar{\psi}(A) \cdot u_\psi = \sum_{A \in \mathrm{Cl}^+} \frac{2}{h^+} \sum_{\psi \text{ odd}} \bar{\psi}(A)\psi(A) \cdot u_A = \sum_{A \in \mathrm{Cl}^+} \mathbf{1}_A^* \cdot u_A = u_A \cdot u_{A[\sqrt{D}]}^{-1}. \tag{2.22}$$

The condition $\bar{u}_A = 1/u_A$ is equivalent to $u_{A[\sqrt{D}]} = u_A^{-1}$, so $\frac{2}{h^+} \sum_{\psi \text{ odd}} \frac{1}{2} \log_p u_\psi = \log_p(u_A)$. □

This gives a reasonably efficient algorithm for computing $\log_p u_A$, described in algorithm 2. The step `KatzBasis` is described in step 3 of [**Lau11**, Algorithm 1]. Roughly speaking, a Katz basis form is the ratio of a classical modular form of weight $2 + (p-1)i$ and E_{p-1}^i. Computing finitely many of these to sufficiently high finite precision, these span a subspace of $M_2^\dagger(\mathrm{SL}_2(\mathbb{Z}))$ in which we can uniquely detect ∂f_Q^+. Further details and proofs can be found in [**Kat73**, Chap. 2].

The function `FindConstTerm` first solves a linear system obtained by solving for the higher order coefficients of ∂f_Q^+ in terms of those in B, so that the constant

Algorithm 2: Algorithm for computing $\log_p u_A$.

Input: A real quadratic field $F = \mathbb{Q}(\sqrt{D})$, a rational prime p inert in F, a class $A \in \mathrm{Cl}^+$ represented by a reduced quadratic form Q_0, and an integer N.
Output: $\log_p u_A$ as an element of F_p to p-adic precision N.

$m \leftarrow p \cdot N$
Compute $\{M(n, A)\}_{n \leq m}$ using Algorithm 1
Compute $\{a_n(\partial f_Q^+)\}_{n \leq m}$ using Equation (2.21)
$B \leftarrow \texttt{KatzBasis}(M_2^\dagger(\mathrm{SL}_2(\mathbb{Z})) \bmod p^N, q^m)$
$\log_p u_A \leftarrow \texttt{FindConstTerm}(\{a_n\}_{n \leq m}, B)$
return $\log_p u_A \bmod p^N$

term of ∂f_Q^+ is a linear combination of the constant terms of the Katz basis forms. The number of terms m computed in the q-expansion of ∂f_Q^+ ensures that it can always be found in the Katz basis from [**Lau11**, Algorithm 1], although in practice smaller values of m are often sufficient.

With a little extra work we can compute the spectral expansion of $e_{\mathrm{ord}}(\partial f_Q^+)$. To compute the ordinary projection, we use a trick due to Lauder. The idea is to compute a matrix for the U_p-operator acting on the Katz basis B from Algorithm 2, computed to precision $\dim M_{k'}(\mathrm{SL}_2(\mathbb{Z}))$, where $k' := 2 + (p-1)\lfloor N(p+1)/p \rfloor$. Since this approximate basis is finite, the matrix U_p has finite rank. Raising the matrix to the power $2m$ and applying to the vector defining ∂f_ψ^+ then gives the ordinary projection. We denote this step by `OrdinaryProjection` in Algorithm 3. Here $\texttt{FindInSpace}(G, M)$ solves for $G = e_{\mathrm{ord}}(\partial f_Q^+)$ in terms of the eigenbasis for

Algorithm 3: Algorithm for the spectral expansion of $e_{\mathrm{ord}}(\partial f_Q^+)$.

Input: A real quadratic field $F = \mathbb{Q}(\sqrt{D})$, a rational prime p inert in F, a character $\psi\colon \mathrm{Cl}^+ \to \mathbb{C}^\times$ and a positive integer m.
Output: The coefficients λ_0 and λ_f of $e_{\mathrm{ord}}(\partial f_\psi^+)$ as elements of F_p, represented with p-adic precision N.

$m \leftarrow \dim M_{2+(p-1)\lfloor N(p+1)/p \rfloor}(\mathrm{SL}_2(\mathbb{Z}))$
Compute $B \bmod (p^m, q^N)$ and $\{a_n(\partial f_\psi^+)\}_{n=0}^N$ as in Algorithm 2
$G \leftarrow \texttt{OrdinaryProjection}(\{a_n(\partial f_\psi^+)\}_{n=0}^N, B)$
$M \leftarrow M_2(\Gamma_0(p)) \otimes F_p$
return `FindInSpace(G, M)`

$M_2(\Gamma_0(p))$ and returns the corresponding coefficients, which are precisely λ_0 and the λ_f for eigenforms f. The same algorithm works for $e_{\mathrm{ord}}(\partial f_\psi^+)$.

3. From logarithms to invariants

In this section we explain how to recover u_A from $\log_p u_A$ and $P_{\psi,f}$ from λ_f.

29 Jun 2023 06:07:20 PDT
230121-Damm Version 2 - Submitted to LuCaNT

3.1. Recovering a Gross–Stark unit from its p-adic logarithm. The "virtual units" u_A are difficult to work with because they are formal powers of units in H, and thus do not have a unique minimal polynomial. Instead, we use the Brumer–Stark conjecture and look instead for the (conjectural) element $\epsilon_A \in \mathcal{O}_H^\times[1/p]$ satisfying $e \cdot u_A = \epsilon_A \otimes 1$, where $e := \#\mu(H)$. This property implies that $\log_p u_A = \frac{1}{e} \log_p \epsilon_A$. Note that while u_A is determined uniquely by Equation (2.2) because $\mathcal{O}_H^\times[1/p] \otimes \mathbb{Q}$ is torsion-free, ϵ_A is only unique up to roots of unity in H. This ambiguity is natural for several reasons. First, the Brumer–Stark units over $\mathbb{Q}$ constructed in [**Gro81**] are Gauss sums, which by definition require a choice of a root of unity to determine the additive character. Second, ϵ_A being defined only up to torsion in $\mathcal{O}_H^\times[1/p]$ mirrors the fact that Stark–Heegner points are defined up to torsion in $E(H)$.

We can find the exact value of e without computing the unit group of $\mathcal{O}_H$ directly by noting that any root of unity in H will lie in the *genus field* of F, the largest subextension of H which is abelian over $\mathbb{Q}$. This has the following classical description:

Proposition 3.1 ([**Lem00**, Prop. 2.19])**.** *Let $F = \mathbb{Q}(\sqrt{D})$, and let $D = D_1 \cdots D_t$ be the factorisation of D into prime discriminants, meaning each D_i is either -4, -8, 8 or $(-1)^{(p-1)/2}p$ for an odd prime p. Then the genus field of F equals $\mathbb{Q}(\sqrt{D_1}, \dots, \sqrt{D_t})$.*

Since the only quadratic extensions with other roots of unity than ± 1 are $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, we obtain the following:

Corollary 3.2. *We have $\#\mu(H) > 2$ if and only if either of the following holds:*

(1) $D \equiv 0 \bmod 3$*, in which case H contains a cube root of unity.*
(2) $D \equiv 0 \bmod 4$ *and* $D/4 \equiv 3 \bmod 4$*, in which case H contains $\sqrt{-1}$.*

The kernel of $\log_p$ is much larger than that of the archimedean log, containing powers of p as well as roots of unity. Passing from $\log_p \epsilon_A$ to ϵ_A requires knowing both $\mathrm{ord}_{\mathfrak{P}} \epsilon_A$ and $\epsilon_A \bmod \mathfrak{P}$. We can deal with the latter by looping through all the roots of unity in $H_{\mathfrak{P}}$, of which there are $p^2 - 1$, and test each product separately. This, along with the computation of the Katz basis, are the main bottlenecks in the algorithm for large values of p. Certain Stark units modulo p appear in a recent conjecture of Harris–Venkatesh [**HV19**], and it would be interesting to see if an analogous conjecture could describe the mod $\mathfrak{P}$ reduction of u_A.

To find the $\mathfrak{P}$-valuation, we use a classical theorem due to C. Meyer which we now describe. Let $A \in \mathrm{Cl}^+$ be a narrow ideal class, and recall that the corresponding partial ζ-function is given by

$$\zeta(s, A) := \sum_{\mathfrak{a} \leq \mathcal{O}_F,\, [\mathfrak{a}] = A} \frac{1}{N(\mathfrak{a})^s}, \qquad \mathrm{Re}(s) > 1. \tag{3.1}$$

Let $\zeta_-(s, A) := \frac{1}{2}(\zeta(s, A) - \zeta(s, A[(\sqrt{D})]))$. This is non-zero if and only if F has no unit of negative norm, which is our running assumption.

Let η denote the fundamental unit of F, by assumption satisfying $N(\eta) = 1$, and fix a representative $\mathfrak{a} \leq \mathcal{O}_K$ for A with $\mathbb{Z}$-basis $1, w$. Then $\eta \cdot \mathfrak{a} = \mathfrak{a}$, and so we can find integers a, b, c and d such that

$$\epsilon w = aw + b \quad \text{and} \quad \epsilon = cw + d.$$

29 Jun 2023 06:07:20 PDT
230121-Damm Version 2 - Submitted to LuCaNT

This is done explicitly in Algorithm 4. Since the action of η is invertible and preserves the order of the basis, the matrix $\gamma_A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has determinant 1. Passing to the quadratic form $Q = Q_1x^2 + Q_2xy + Q_3y^2$ associated to $\mathfrak{a}$ by Proposition 2.3 and writing $\eta = u + t\sqrt{D}$, a straightforward computation shows that

$$\gamma_A = \begin{pmatrix} t + Q_2u & 2Q_3u \\ -2Q_1u & t - Q_2u \end{pmatrix}. \tag{3.2}$$

Let $\Phi\colon \mathrm{SL}_2(\mathbb{Z}) \to \mathbb{R}$ denote the *Dedekind symbol* defined by

$$\Phi\begin{pmatrix} a & b \\ c & d \end{pmatrix} := \begin{cases} b/d & \text{if } c = 0, \\ \frac{a+d}{c} - 12\,\mathrm{sgn}(c)\cdot s(a,c) & \text{if } c \neq 0, \end{cases} \tag{3.3}$$

where $s(a,c)$ is the *Dedekind sum*

$$s(a,c) := \sum_{k=1}^{|c|} \left(\left(\frac{ak}{c}\right)\right)\left(\left(\frac{k}{c}\right)\right) \quad \text{for} \quad (a,c) = 1, c \neq 0, \tag{3.4}$$

with $((x)) = 0$ if $x \in \mathbb{Z}$ and $((x)) = x - \lfloor x \rfloor - 1/2$ otherwise.

By adding a correction term to Φ, Rademacher showed that the eponymous *Rademacher symbol*,

$$\Psi(\gamma) := \Phi(\gamma) - 3\,\mathrm{sgn}(c(a+d)), \tag{3.5}$$

depends only on the conjugacy class of γ.

THEOREM 3.3 (Meyer). *Fix a class $A \in \mathrm{Cl}^+$, and let $\gamma_A \in \mathrm{SL}_2(\mathbb{Z})$ be the associated matrix. Then*

$$\zeta_-(0,A) = \frac{1}{12}\Psi(\gamma_A). \tag{3.6}$$

This follows from a version of Kronecker's limit formula for real quadratic fields, and the proof is described in [**DIT18**].

Corollary 3.4. *Let u_A be a Gross–Stark unit attached to a narrow ideal class A. Then*

$$\mathrm{ord}_{\mathfrak{P}}\, u_A = -\frac{1}{12}\Psi(\gamma_A). \tag{3.7}$$

Similarly, for the associated Brumer–Stark unit ϵ_A,

$$\mathrm{ord}_{\mathfrak{P}}\, \epsilon_A = -\frac{e}{12}\Psi(\gamma_A), \tag{3.8}$$

where $e = \#\mu(H)$.

PROOF. By Equation (2.2),

$$\mathrm{ord}_{\mathfrak{P}}\, u_A = \frac{1}{2}(\mathrm{ord}_{\mathfrak{P}}\, u_A - \mathrm{ord}_{\mathfrak{P}}\, u_{A[\sqrt{D}]}) \tag{3.9a}$$

$$= -\frac{1}{2}(\zeta(0,A) - \zeta(0,A[\sqrt{D}]) \tag{3.9b}$$

$$= -\zeta_-(0,A) = -\frac{1}{12}\Psi(\gamma_A). \tag{3.9c}$$

The second claim follows immediately from the identity $e \cdot u_A = \epsilon_A \otimes 1$. □

Algorithm 4: Compute $\operatorname{ord}_{\mathfrak{P}} \epsilon_A$ using Meyer's formula.

Input: An indefinite binary quadratic form $Q(x,y) = Q_1x^2 + Q_2xy + Q_3y^2$ of square-free discriminant D, representing a narrow ideal class A of $F = \mathbb{Q}(\sqrt{D})$.
Output: $\operatorname{ord}_{\mathfrak{P}} \epsilon_A$.

$t, u \leftarrow$ `PellSolution`(D) `// Solve Pell's equation in` $\mathbb{Q}(\sqrt{D})$ `to find fundamental unit` $\epsilon = u + t\sqrt{D}$.

$\gamma_A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \leftarrow \begin{pmatrix} t + Q_2u & 2Q_3u \\ -2Q_1u & t - Q_2u \end{pmatrix}$
if $c = 0$ **then**
  $\Phi \leftarrow b/d$
else
  $\Phi \leftarrow \frac{a+d}{c} - 12\operatorname{sgn}(c) \cdot$ `DedekindSum`(a, c)
$\Psi \leftarrow \Phi - 3\operatorname{sgn}(c(a+d))$
return $-e \cdot \Psi/12$

Algorithm 4 describes how to efficiently compute $\operatorname{ord}_{\mathfrak{P}} \epsilon_A$ using Meyer's theorem.

The fundamental solution of Pell's equation grows very quickly as D gets large, so computing Dedekind sums by evaluating Equation (3.4) directly can be very slow for large values of D. Instead we use a formula from [**Apo90**, Ex. 3.10]: By replacing c by $-c$ and a by $a \bmod c$, we can assume that $0 < a < c$. Let $r_0 := c$, $r_1 := a$ and define r_j recursively to be the remainders in the Euclidean algorithm applied to a and c, satisfying $r_{j+1} \equiv r_{j-1} \bmod r_j$ and $1 = r_{n+1} < \dots r_{j+1} < r_j \dots < r_0$ for all $1 \leq j \leq n-1$. Then

$$s(a,c) = \frac{1}{12} \sum_{j=1}^{n+1} \left(\frac{r_j^2 + r_{j-1}^2 + 1}{r_j r_{j-1}} \right) - \frac{(-1)^n + 1}{8}. \tag{3.10}$$

This is very efficient in practice.

Remark 3.5. It is also possible to compute the value of $\zeta_-(0, A)$ using a theorem due to Zagier, [**Zag81**, §14, Satz 2], which expresses $\zeta_-(0, A)$ as an elementary sum of numbers appearing in the reduction algorithm for indefinite quadratic forms. We thank an anonymous referee for pointing this out. Having implemented both Zagier reduction and Algorithm 4 in the `sage` library, we see that Zagier's formula is much faster in practice. However, if we compute the automorph using reduction theory instead of by solving Pell's equation, then the algorithms perform roughly equally well.

By the *minimal polynomial of* ϵ we mean the irreducible polynomial P of minimal degree satisfying $P(\epsilon) = 0$ with coefficients in $\mathcal{O}_F$ not all divisible by the same prime, such that the leading term is a positive power of p.

Lemma 3.6. *Let ϵ be a Brumer–Stark unit in $\mathcal{O}_H[1/p]^\times$, and let $P(T) = \sum_{i=0}^d a_i T^i = a_d \prod_{\sigma \in G}(T - \sigma(\epsilon))$ be its minimal polynomial. Then*

(1) *ϵ is a primitive element of H over F, $H = F(\epsilon)$.*
(2) *P is of degree h^+, and after possibly twisting ϵ by a root of unity in H, has rational integer coefficients.*
(3) *P is reciprocal, $a_i = a_{d-i}$ for all $0 \le i \le d$.*

Proof. (i) We follow the strategy of [**Rob97**, Théorème 2.3]. Suppose $\sigma(\epsilon) = \epsilon$ for some $\sigma \in G$. For any character $\chi\colon G \to \mathbb{C}^\times$, let $L_S(s,\chi)$ denote the L-function of χ with the Euler factor at $\mathfrak{p} = (p) \subset \mathcal{O}_F$ removed. Since $\sigma_\mathfrak{p} = 1$, $\chi(\sigma_\mathfrak{p}) = 1$, and so we have $L_S(0,\chi) = 0$. A consequence of the Brumer–Stark conjecture, see for example [**Tat81**, Prop. (5.5) and Conj. (4.2)], is that ϵ satisfies

$$L'_S(0,\chi) = -\frac{1}{e}\sum_{\sigma' \in G} \chi(\sigma') \log|\sigma'(\epsilon)|_\mathfrak{P} \tag{3.11}$$

for all χ. It follows that

$$L'_S(0,\chi) = -\frac{1}{e}\sum_{\sigma' \in G} \chi(\sigma') \log|\sigma'(\epsilon)|_\mathfrak{P} \tag{3.12a}$$

$$= -\frac{1}{e}\sum_{\sigma' \in G} \chi(\sigma') \log|\sigma'\sigma(\epsilon)|_\mathfrak{P} \tag{3.12b}$$

$$= -\frac{\bar{\chi}(\sigma)}{e}\sum_{\sigma'' \in G} \chi(\sigma'') \log|\sigma''(\epsilon)|_\mathfrak{P} \tag{3.12c}$$

$$= \bar{\chi}(\sigma) L'_S(0,\chi). \tag{3.12d}$$

If χ is odd, then $L'_S(0,\chi) \neq 0$ by [**Gro81**, Eq. 3.1], so $\sigma \in \bigcap_{\chi \text{ odd}} \ker\chi$. Fix an odd character ψ, and note that there is a bijection between even characters χ and the set of characters $\psi \cdot \psi'$ where ψ' runs over all odd characters. Now

$$\sum_{\chi \in \hat{G}} \chi(\sigma) = \sum_{\chi \text{ odd}} \chi(\sigma) + \sum_{\chi \text{ even}} \chi(\sigma) = (1 + \psi(\sigma)) \sum_{\psi' \text{ odd}} \psi'(\sigma) = 2\#\{\chi \text{ odd}\} = h^+, \tag{3.13}$$

and so $\sigma = 1$.

(ii) The degree of P is h^+ since ϵ is primitive. Let τ be an RM-point in the sense of [**DPV23**]. As described in [**DV21**, §3.2], $\mathrm{Gal}(H/\mathbb{Q}) \cong \mathrm{Gal}(H/F) \rtimes \mathrm{Gal}(F/\mathbb{Q})$, and we can identify the image of the generator of $\mathrm{Gal}(F/\mathbb{Q})$ with $\sigma_\mathfrak{P}$.

By the Shimura reciprocity conjecture [**DV21**, Conj. 3.14], $\sigma_\mathfrak{P}(J_{\mathrm{DR}}[\tau]) = J_{\mathrm{DR}}[\tau']$. If we let τ be the RM point corresponding to the identity class in Cl^+, then $J_{\mathrm{DR}}[\tau] = J_{\mathrm{DR}}[\tau']$, and so $J_{\mathrm{DR}}[\tau]$ is fixed by $\sigma_\mathfrak{P}$. Thus the minimal polynomial of $J_{\mathrm{DR}}[\tau]$ is fixed by $\sigma_\mathfrak{P}$, and as ϵ_A is a conjugate of $J_{\mathrm{DR}}[\tau]$ up to roots of unity in H, the result follows.

(iii) P being reciprocal is equivalent to $P(T) = T^d P(1/T)$, which is true if for any non-zero root v of P, $1/v$ is also a root of P. But with κ denoting complex conjugation in G, Equation (2.2) implies $\kappa(\sigma(\epsilon)) = 1/\sigma(\epsilon)$. □

Knowing the $\mathfrak{P}$-valuations of all the conjugates of ϵ lets us bound the valuations of the coefficients of P:

Lemma 3.7. *Let $v_0 \ldots, v_{d/2-1}$ be the $\mathfrak{P}$-valuations of the conjugates of ϵ which are positive, ordered so that $v_0 \ge v_1 \ge \ldots \ge v_{d/2-1} \ge 0$, and $v_{d/2} = 0$. Then for any $i = 0, \ldots, d/2$ we have $\mathrm{ord}_p(a_i) \ge \sum_{j=0}^{d/2-i} v_{d/2-j}$. In particular, $\mathrm{ord}_p(a_d) = \mathrm{ord}_p(a_0) = \sum_{j=0}^{d/2} v_j$.*

PROOF. By Lemma 3.6 (iii), the Newton polygon of P is symmetric around the vertical line $x = d/2$, and its slopes are precisely equal to the p-valuations of the roots of P, the conjugates of u. Since P is normalised, we know that $\operatorname{ord}_p a_{d/2} = 0$, so the Newton polygon of P intersects the x-axis at the point $(0, d/2)$. To estimate the remaining coefficients, note that the Newton polygon of P will always lie in the convex hull of the polygon determined as follows: the boundary is symmetric around the line $x = d/2$, and is determined by the points $(i, \sum_{j=0}^{d/2-i} v_j)$ for $0 \le i \le d/2$. Since the y-coordinate of a point determining the Newton polygon of P is the $\mathfrak{P}$-valuation of the corresponding coefficient, this gives the required inequality. $\square$

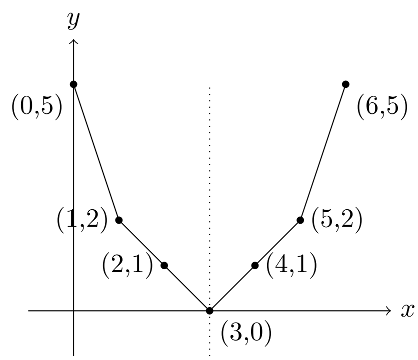

FIGURE 1. The largest possible Newton polygon determined by the $\mathfrak{P}$-valuations of the conjugates of a Brumer–Stark unit over $\mathbb{Q}(\sqrt{469})$, where the vector of valuations is given by $(-3, -1, -1, 1, 1, 3)$.

Let $\alpha = (\alpha_1, \alpha_2) \in \mathbb{Z}/p^m \times \mathbb{Z}/p^m$ be an approximation of $\exp_p(\log_p \epsilon_A)$, where for a fixed generator s of $\mathbb{Q}_{p^2}$ over $\mathbb{Q}_p$ we define the natural map

$$\mathbb{Z}_{p^2} = \mathbb{Z}_p[s] \to \mathbb{Z}/p^m \times \mathbb{Z}/p^m \quad \text{by} \quad a + bs \mapsto (a \bmod p^m, b \bmod p^m). \tag{3.14}$$

To find the minimal polynomial P of α, we apply the `LLL` algorithm to look for linear integral relations between powers of α. This is a common application of the LLL algorithm, and a more detailed exposition can be found in [**Coh93**, §2.7.2]. Roughly speaking, the `LLL` algorithm takes as input a basis $b_1, \dots, b_d$ for a Euclidean lattice $\Lambda \subset \mathbb{R}^n$, and returns a "better" basis $b_1^*, \dots, b_d^*$ for Λ, in the sense that b_1^* has relatively small norm and that the vectors are approximately orthogonal. Let $v_0, \dots, v_{d/2-1}$ be the $\mathfrak{P}$-valuations of the conjugates of ϵ ordered as in Lemma 3.7, computed using Algorithm 4. We want to find a short nontrivial vector in the lattice spanned by the rows of the following $(d/2+3) \times (d/2+3)$-matrix:

$$\begin{pmatrix}
1 & 0 & \dots & 0 & p^{v_0}(1+\alpha^d)_1 & p^{v_0}(1+\alpha^d)_2 \\
0 & 1 & \dots & 0 & p^{v_1}(\alpha^1+\alpha^{d-1})_1 & p^{v_1}(\alpha^1+\alpha^{d-1})_2 \\
0 & 0 & \dots & 0 & p^{v_2}(\alpha^2+\alpha^{d-2})_1 & p^{v_2}(\alpha^2+\alpha^{d-2})_2 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & \dots & 1 & (\alpha^{d/2})_1 & (\alpha^{d/2})_2 \\
0 & 0 & \dots & 0 & p^m & 0 \\
0 & 0 & \dots & 0 & 0 & p^m
\end{pmatrix} \tag{3.15}$$

A vector

$$w = \Big(n_0, \ldots, n_{d/2}, n_{d/2}\alpha_1^{d/2} + \sum_{i=0}^{d/2-1} p^{v_i} n_i(\alpha^i + \alpha^{d-i} + p^m)_1, \\ n_{d/2}\alpha_2^{d/2} + \sum_{i=0}^{d/2-1} p^{v_i} n_i(\alpha^i + \alpha^{d-i} + p^m)_2\Big), \tag{3.16}$$

in the lattice is small only if $n_{d/2}\alpha^{d/2} + \sum_{i=0}^{d/2-1} p^{v_i} n_i(\alpha^i + \alpha^{d-i}) \equiv 0 \bmod p^m$. Then the polynomial $\sum_{i=0}^{d/2} p^{v_i} n_i x^i + \sum_{i=d/2+1}^{d} p^{v_{d/2-i}} n_{d-i} x^i$ is a good candidate for the minimal polynomial of P over $\mathbb{Q}$. This suggests the following algorithm:

Algorithm 5: Find the minimal polynomial of ϵ_A from the p-adic approximation of $\log_p \epsilon_A$.

Input:
- $\alpha \in \mathbb{Q}_{p^2}$ an approximation to $\exp_p(\log_p \epsilon_A)$,
- $v_0, \ldots, v_{d/2-1}$ as in Lemma 3.7.

Output: The minimal polynomial $P \in \mathbb{Z}[x]$ of ϵ_A.

$\zeta \leftarrow$ primitive (p^2-1)-st root of unity in $\mathbb{Q}_{p^2}$
for $k = 0$ *to* $p^2 - 1$ **do**
    $\alpha' \leftarrow \zeta^k \alpha$
    $M \leftarrow$ matrix described in Equation (3.15) with α' in place of α
    $v = (n_i) \leftarrow$ first vector returned by `LLL`(M)
    $P \leftarrow \sum_{i=0}^{d/2} n_i x^i + \sum_{i=d/2+1}^{d} n_{d-i} x^i$
    if $n_0 = p^r$ *for some* $r \in \mathbb{N}$ **then**
        if `IsBSUnitCharPoly`(P) **then** `// Described below`
            return P.
return 0

In practice, it is convenient to pick $A \in \mathrm{Cl}^+$ so that $\mathrm{ord}_{\mathfrak{P}}\, \epsilon_A$ is as close to 0 as possible. A similar algorithm for recognising an algebraic number from a p-adic approximation is given in [**GHK**$^+$**06**, §4.2].

The function `IsBSUnitCharPoly` performs a series of tests in order, and returns `False` if any test fails:

(1) if P is irreducible over F, hence generates an extension of F of degree h^+,
(2) if the absolute discriminant of $H' := F[x]/(P(x))$ is a power of D, which is equivalent to H'/F being unramified at all finite places,
(3) if H'/F is abelian.
At this point we know that $H' \cong H$, but to ensure that P is the minimal polynomial of a Brumer–Stark unit and not just any generator of H, we perform a further test:
(4) test if the extension generated by $P(x^e)$ is a central extension.

If all of these tests are passed, then it is quite likely, although not absolutely certain, that the polynomial P has a Brumer–Stark unit as a root. To be absolutely certain, one should test if $P(x^e)$ generates an abelian extension of F, but this is computationally unfeasible when both h and e are large.

Remark 3.8. The requirement that the extension should be central was part of Stark's original conjecture, see [**Sta80**, Conj. 1], and in [**PRS11**, p. 40] Stark notes that this was sufficient for the factorisation of regulators which motivated it. The condition that the extension should be in fact be abelian was observed by Tate, leading to the formulation of the Brumer–Stark conjecture. This is now known to be true, by the work of Dasgupta and Kakde [**DK23**].

It would be interesting to know whether "central implies abelian" in this situation, that is: if α is a p-unit which generates H with $\mathfrak{P}^\sigma$-valuations specified by Equation (3.8) and $\sqrt[e]{\alpha}$ generates a central extension of F, is the extension actually abelian?

To describe the test in (4), it is convenient to introduce some notation: Let $K := H(\sqrt[e]{\epsilon_A})$ and $G_e := \mathrm{Gal}(K/H)$. By Kummer theory, $G_e \cong \mathbb{Z}/e\mathbb{Z}$. In this case $\Gamma := \mathrm{Gal}(K/F)$ is a group extension of G_e and G,

$$1 \to G_e \to \Gamma \to G \to 1. \tag{3.17}$$

The following lemma gives a simple criterion for deciding whether Γ is a central extension, that is, if G_e lies in the centre of Γ, without computing Γ directly:

Lemma 3.9. *Let F be a number field, H/F a Galois extension containing all e-th roots of unity, and $\alpha \in H^\times$. Define $\chi_{\mathrm{cyc}} \colon G := \mathrm{Gal}(H/F) \to (\mathbb{Z}/e\mathbb{Z})^\times$ by $\zeta^{\chi_{\mathrm{cyc}}(\sigma)} = \sigma(\zeta)$ for any $\zeta \in \mu_e(H)$. Then $K := H(\sqrt[e]{\alpha})/F$ is a central extension if and only if for all $\sigma \in G$ there exists some $\beta \in H^\times$ such that $\sigma(\alpha) = \alpha^{\chi_{\mathrm{cyc}}(\sigma)}\beta^e$.*

Proof. There is a natural action of G on $G_e := \mathrm{Gal}(K/H)$ by conjugation, $\sigma \cdot g := \sigma g \sigma^{-1}$, which is well-defined precisely because G_e is abelian. The extension K/F is central if and only if the action is trivial. Let Δ be a set of representatives of $H^\times/(H^\times)^e$, and note that this admits a natural action of G. The Kummer pairing ([**Gra03**, §I.6]) gives a G-equivariant isomorphism $G_e \cong \mathrm{Hom}(\Delta, \mu_e(K))$. The action of G_e on the right-hand side is given by $(\sigma \cdot \phi)(\alpha) = \phi(\sigma^{-1}(\alpha))^{\chi_{\mathrm{cyc}}(\sigma)}$, where $\chi_{\mathrm{cyc}}(\sigma)$ is defined by $\sigma \cdot \zeta_e = \zeta_e^{\chi_{\mathrm{cyc}}(\sigma)}$. The action of G on G_e is trivial if and only if the action on $\mathrm{Hom}(\Delta, \mu_e)$ is trivial. Each element of this group is given by $\psi_g \colon \delta \mapsto \langle \delta, g\rangle := \frac{g\sqrt[e]{\delta}}{\sqrt[e]{\delta}}$ for some $g \in G_e$, and so Γ is central if and only if $(\sigma \cdot \psi_g)(\delta) = \psi_g(\delta)$ for all $\delta \in \Delta$, $g \in G_e$ and $\sigma \in G$. Equivalently,

$$\left(\frac{g\sqrt[e]{\sigma^{-1}(\delta)}}{\sqrt[e]{\sigma^{-1}(\delta)}}\right)^{\chi_{\mathrm{cyc}}(\sigma)} = \frac{g\sqrt[e]{\delta}}{\sqrt[e]{\delta}} \quad \text{hence} \quad g\left(\sqrt[e]{\frac{\alpha^{\chi_{\mathrm{cyc}}(\sigma)}}{\sigma(\alpha)}}\right) = \sqrt[e]{\frac{\alpha^{\chi_{\mathrm{cyc}}(\sigma)}}{\sigma(\alpha)}}, \tag{3.18}$$

where $\alpha := \sigma^{-1}(\delta)$. This being true for all g is equivalent to $\frac{\alpha^{\chi_{\mathrm{cyc}}(\sigma)}}{\sigma(\alpha)}$ being an e-th power for all σ. Finally, note that G acts transitively on Δ, so it suffices to check the criterion for a single α. $\square$

This test can be implemented quite easily, and is mainly bottlenecked by the computation of $\mathrm{Gal}(H/F)$, at least when $[H : F]$ is reasonably large.

Remark 3.10. A test for whether an extension is abelian is found in [**Coh12**, Algorithm 4.4.6]. In short, the Takagi existence theorem gives a bijection between abelian extensions K/F and certain *Takagi subgroups* of a ray class group $\mathrm{Cl}_{\mathfrak{m}} F$, where $\mathfrak{m}$ is a sufficiently large modulus. However, this is very slow when e and h are large, because it requires computing the ray class group of F of modulus equal to the relative discriminant of $H(\sqrt[e]{\alpha})/F$, which is relatively large.

3.2. Detecting Stark–Heegner points. Our method of finding Stark–Heegner points is much more primitive, because we don't have an equivalent of the Brumer–Stark conjecture.

Let $E/\mathbb{Q}$ be an elliptic curve with split multiplicative reduction at p. Recall from Theorem 2.2 that if E has associated eigenform $f \in M_2(\Gamma_0(p))$, then the corresponding spectral coefficient $\lambda_f = -L_{\text{alg}}(1, f) \log_E(P_{\psi,f})$ involves a point $P_{\psi,f}$ conjecturally defined over H. To find this, we make use of the Tate curve E_q isomorphic to E, which is described explicitly with the formulae in [**Sil09**, §C.14]. From this we can find an explicit isomorphism $F_p^\times/q^\mathbb{Z} \xrightarrow{\phi} E_q(F_p)$, where q is an element satisfying $|q| < 1$ generating a discrete subgroup. An approximation to $\alpha \coloneqq \exp_p(-\lambda_f/L_{\text{alg}}(1, f))$ can then be mapped to a point on the Tate curve $E_q(F_p)$. Mapping further into $E(F_p)$, we may compute using descent a generating set $\{g\}$ for $E(H)$ and attempt to write the image of α as an integral combination of them. Since $P_{\psi,f}$ is only defined up to torsion, it is reasonable to look for a dependence between the formal logarithms of α and the generators $\{g\}$. To ensure convergence of the corresponding power series, we replace α by α^{p-1} and each g by $(p-1)g$. Then we look for an integer relation by applying the `LLL`-algorithm to a suitable lattice as in the previous section. Following the convention in `pari/gp`, we call this step `lindep`.

In summary, we have Algorithm 6.

Algorithm 6: Find Stark–Heegner point $P_{\psi,f}$ from λ_f.

Input:
- A normalised eigenform f in $M_2(\Gamma_0(p))$ with Hecke field $\mathbb{Q}$,
- an elliptic curve E with associated eigenform f,
- $\lambda_f \in (\mathbb{Z}/p^m\mathbb{Z})^2$ an approximation to $-L_{\text{alg}}(1, f) \log_{E_f}(P_{\psi,f}) \in F_p$.

Output: The point $P_{\psi,f}$ on the elliptic curve E

$E_q \leftarrow$ `TateCurve`(E) `// Using formulae in [Sil09, §C.14]`
$\phi \leftarrow$ `Isomorphism`$(F_p^\times/q^\mathbb{Z}, E_q)$ `// As in [Sil09, Thm. 14.1]`
$\beta \leftarrow \phi(-\lambda_f/L_{\text{alg}}(1, f))$
$H \leftarrow$ `NarrowHilbertClassField`(F)
$E(H) \leftarrow$ `MordellWeilGroup`(E/H)
$L \leftarrow [\log_{E_q}((p-1)\beta)]$
`// Compute formal logarithms of non-torsion generators of` $E(H)$`:`
for $g \in$ `Generators`$(E(H))$ **do**
  if `Order(g)` $==$ `0` **then**
    $L \leftarrow L \cup \{\log_E((p-1)g)\}$
$(n_1, (n_g)) \leftarrow$ `lindep`(L) `// Find integer relation between formal logarithms using LLL.`
return $\sum_g n_g \cdot g/n_1 \in E(H)$

By linearity, the algorithm works equally well when λ_f comes from ∂f_Q^+, in which case the corresponding Stark–Heegner point is a weighted sum of points $P_{\psi,f}$. The algebraic part of the L-value can be computed either directly in `magma` using the intrinsic `LRatio`, or by using the BSD formula and the invariants of E since $L(s,f) = L(s,E)$, or even analytically by approximating $L(1,E)$ and computing the periods of E.

One limitation of Algorithm 6 is that computing $E(H)$ is very slow when $[H : \mathbb{Q}] > 4$. We hope to resolve this in the future by improving the algorithms for detecting polynomials from p-adic approximations to their roots.

In the table below we have computed the minimal polynomials of the X and Y coordinates of the Stark–Heegner points coming from ∂f_ψ^+ on the curve $E : y^2+xy+y = x^3-x^2-x-14$. This is a model for $X_0(17)$, for which we have $L_{\mathrm{alg}}(1,f) = 1/4$, so $\lambda_f = -\frac{1}{4}\log_E P_{\psi,f}$. Here ψ denotes the genus character associated with $\mathbb{Q}(\sqrt{D})$: since all the fields $\mathbb{Q}(\sqrt{D})$ for $D < 100$ with no fundamental unit of negative norm such that $\left(\frac{D}{17}\right) = -1$ have narrow class number 2, there is a unique nontrivial character. This satisfies $\partial f_\psi^+ = -\partial f_Q^+$, where Q is a quadratic form with class corresponding to the inverse different in Cl^+. Note that this matches the table on p. 545 of [**DPV21**].

Table 2. Table of Stark–Heegner points on $E : y^2 + xy + y = x^3 - x^2 - x - 14$, for $D < 100$.

D	X	Y
12	$x^2 - 6x + 10$	$x^2 - 2x + 10$
24	$x^2 + \frac{2}{9}x + \frac{89}{9}$	$x^2 + \frac{230}{27}x + 25$
28	$x^2 - 6x + 10$	$x^2 + 10x + 41$
44	$x^2 - 14x + 338$	$x^2 - 26x + 7394$
56	$x^2 + \frac{2}{9}x + \frac{89}{9}$	$x^2 + \frac{230}{27}x + 25$
57	$x^2 + \frac{2306}{1225}x + \frac{6521}{1225}$	$x^2 + \frac{111042}{42875}x + \frac{15319}{8575}$
88	$x^2 + \frac{2}{9}x + \frac{89}{9}$	$x^2 - \frac{182}{27}x + \frac{401}{9}$
92	$x^2 - 6x + 10$	$x^2 - 2x + 10$

3.3. Tables of Brumer–Stark units. Below we show some tables of minimal polynomials of Brumer–Stark units in different ranges. Full tables are in the author's `github` repository, `https://github.com/havarddj/drd`.

Table 3. Minimal polynomials of Brumer–Stark units for $p = 3$, $D < 330$.

D	P_D	D	P_D	D	P_D
44	$3x^2 + 5x + 3$	152	$3x^2 + 2x + 3$	236	$27x^2 + 5x + 27$
56	$3x^2 + 2x + 3$	161	$27x^2 + 38x + 27$	248	$27x^2 - 46x + 27$
77	$3x^2 + 5x + 3$	188	$243x^2 - 298x + 243$	284	$2187x^2 - 4090x + 2187$
92	$27x^2 + 38x + 27$	209	$3x^2 + 5x + 3$	305	$9x^4 + 5x^3 + 17x^2 + 5x + 9$
140	$81x^4 + 6x^3 - 149x^2 + 6x + 81$	221	$9x^4 - 2x^3 - 5x^2 - 2x + 9$	329	$243x^2 - 298x + 243$

Given the data computed, it is natural to study the "horizontal properties" of Brumer–Stark units, meaning the behaviour of the p-units ϵ as elements of $\bar{\mathbb{Q}}$ as D varies.

TABLE 4. Minimal polynomials of Brumer–Stark units for $p = 2$, $2000 \le D \le 2101$.

D	P_D
2005	$2^{12}x^8 + 2^4 \cdot 1055x^7 + 2^2 \cdot 9419x^6 + 57995x^5 + 66831x^4 + 57995x^3 + 2^2 \cdot 9419x^2 + 2^4 \cdot 1055x + 2^{12}$
2013	$2^{30}x^4 - 2^3 \cdot 57677665x^3 - 1118365527x^2 - 2^3 \cdot 57677665x + 2^{30}$
2021	$2^9x^6 + 2^2 \cdot 111x^5 + 2^1 \cdot 123x^4 - 101x^3 + 2^1 \cdot 123x^2 + 2^2 \cdot 111x + 2^9$
2037	$2^{18}x^4 + 2^3 \cdot 16215x^3 - 263887x^2 + 2^3 \cdot 16215x + 2^{18}$
2045	$2^6x^4 - 9x^3 - 65x^2 - 9x + 2^6$
2077	$2^3x^2 + 15x + 2^3$
2085	$2^{24}x^4 - 2^3 \cdot 6289393x^3 + 70333881x^2 - 2^3 \cdot 6289393x + 2^{24}$
2093	$2^8x^4 - 2^1 \cdot 217x^3 + 645x^2 - 2^1 \cdot 217x + 2^8$
2101	$2^{13}x^6 + 2^6 \cdot 79x^5 - 2^3 \cdot 1009x^4 - 10161x^3 - 2^3 \cdot 1009x^2 + 2^6 \cdot 79x + 2^{13}$

The coefficients of the polynomials are all of roughly the same magnitude, despite the strong conditions on the p-valuation of the constant terms. In particular, the logarithmic height of the middle coefficient is roughly $\mathrm{ord}_p\, a_0$, which is easily computed in terms of L-values using Equation (2.2). A classical result of Schur says that the coefficients of cyclotomic polynomials can be arbitrarily large. It would be interesting to know whether the same holds for our polynomials, normalised to be monic. The largest value we find is 822.637, across the tables for $p \in \{2, 3, 5, 7, 11\}$. Figure 2 shows the absolute value of the middle coefficient of the normalised polynomials against the discriminant for different p.

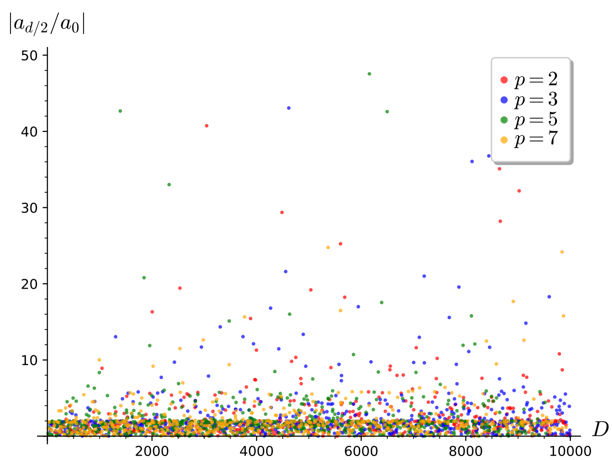

FIGURE 2. Normalised middle coefficients for various primes p.

If we plot the roots of the minimal polynomials on the unit circle as D varies, it is natural to ask how the Brumer–Stark units distribute. It is well-known that the set of Galois orbits of primitive N-th roots of unity becomes equidistributed with respect to the Haar measure as N tends to infinity. One might expect a similar thing to hold for a sequence of Brumer–Stark units, as the size of the corresponding orbits tend to infinity. A weaker statement is that the Brumer–Stark units, for p fixed, become dense in the unit circle as $D \to \infty$.

Questions like these will be addressed in the author's forthcoming DPhil thesis.

References

[Apo90] Tom M. Apostol, *Modular Functions and Dirichlet Series in Number Theory*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1990.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma Algebra System I: The User Language*, Journal of Symbolic Computation **24** (1997), no. 3, 235–265.

[BV07] J. Buchmann and U. Vollmer, *Binary Quadratic Forms: An Algorithmic Approach*, Algorithms and Computation in Mathematics, Springer Berlin Heidelberg, 2007.

[Coh93] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, Springer Berlin Heidelberg, Berlin, Heidelberg, 1993.

[Coh12] ———, *Advanced Topics in Computational Number Theory*, vol. 193, Springer Science & Business Media, 2012.

[Cox11] David A Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, vol. 34, John Wiley and Sons, 2011.

[CR00] Henri Cohen and Xavier-François Roblot, *Computing the Hilbert class field of real quadratic fields*, Mathematics of Computation **69** (2000), no. 231, 1229–1244.

[Dar01] Henri Darmon, *Integration on $Hp \times H$ and Arithmetic Applications*, Annals of Mathematics **154** (2001), no. 3, 589–639.

[Das05] Samit Dasgupta, *Stark-Heegner points on modular Jacobians*, Annales scientifiques de l'École Normale Supérieure **38** (2005), no. 3, 427–469.

[DDP11] Samit Dasgupta, Henri Darmon, and Robert Pollack, *Hilbert Modular Forms and the Gross-Stark Conjecture*, Annals of Mathematics **174** (2011), no. 1, 439–484.

[DG02] Henri Darmon and Peter Green, *Elliptic Curves and Class Fields of Real Quadratic Fields: Algorithms and Evidence*, Experimental Mathematics **11** (2002), no. 1, 37–55.

[DIT18] W. Duke, Ö. Imamoḡlu, and Á. Tóth, *Kronecker's First Limit Formula, Revisited*, Research in the Mathematical Sciences **5** (2018), no. 2, 20.

[DK23] Samit Dasgupta and Mahesh Kakde, *On the Brumer–Stark conjecture*, Annals of Mathematics **197** (2023), no. 1, 289–388.

[DKV18] Samit Dasgupta, Mahesh Kakde, and Kevin Ventullo, *On the Gross-Stark Conjecture*, Annals of Mathematics **188** (2018), no. 3, 833–870.

[DP06] Henri Darmon and Robert Pollack, *Efficient calculation of Stark-Heegner points via overconvergent modular symbols*, Israel Journal of Mathematics **153** (2006), no. 1, 319–354.

[DPV21] Henri Darmon, Alice Pozzi, and Jan Vonk, *Diagonal restrictions of p-adic Eisenstein families*, Mathematische Annalen **379** (2021), no. 1, 503–548.

[DPV23] ———, *The values of the Dedekind–Rademacher cocycle at real multiplication points*, Journal of the European Mathematical Society (2023).

[DV21] Henri Darmon and Jan Vonk, *Singular moduli for real quadratic fields: A rigid analytic approach*, Duke Mathematical Journal **170** (2021), no. 1, 23–93.

[DV22] ———, *Real quadratic Borcherds products*, Pure and Applied Mathematics Quarterly **18** (2022), no. 5, 1803–1865.

[FL22] Max Fleischer and Yijia Liu, *Computation of elliptic units*, https://github.com/liuyj8526/Computation-of-Elliptic-Units, 2022.

[GHK+06] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng, *The 2-Adic CM Method for Genus 2 Curves with Application to Cryptography*, Advances in Cryptology – ASIACRYPT 2006 (Berlin, Heidelberg) (Xuejia Lai and Kefei Chen, eds.), Lecture Notes in Computer Science, Springer, 2006, pp. 114–129.

[GM13] Xavier Guitart and Marc Masdeu, *Computation of {ATR} Darmon Points on Nongeometrically Modular Elliptic Curves*, Experimental Mathematics **22** (2013), no. 1, 85–98.

[GM14] ———, *Overconvergent cohomology and quaternionic Darmon points*, Journal of the London Mathematical Society **90** (2014), no. 2, 495–524.

[GM15] ———, *A p-adic construction of ATR points on $\mathbb{Q}$-curves*, Publicacions Matemàtiques **59** (2015), no. 2, 511–545.

[GMS15] Xavier Guitart, Marc Masdeu, and Mehmet Haluk Sengün, *Darmon points on elliptic curves over number fields of arbitrary signature*, Proceedings of the London Mathematical Society **111** (2015), no. 2, 484–518.

[Gra03] Georges Gras, *Class Field Theory: From Theory to Practice*, Springer Monographs in Mathematics, Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[Gre09] Matthew Greenberg, *Stark-Heegner points and the cohomology of quaternionic Shimura varieties*, Duke Mathematical Journal **147** (2009), no. 3, 541–575.

[Gro81] Benedict H Gross, *p-adic L-series at* $s = 0$, J. Fac. Sci. Univ. Tokyo Sect. IA Math **28** (1981), no. 3, 979–994.

[GZ86] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Inventiones mathematicae **84** (1986), no. 2, 225–320.

[HV19] Michael Harris and Akshay Venkatesh, *Derived Hecke algebra for weight one forms*, Experimental Mathematics **28** (2019), no. 3, 342–361.

[Kat73] Nicholas M. Katz, *p-adic properties of modular schemes and modular forms*, Modular Functions of One Variable III (Berlin, Heidelberg) (Willem Kuijk and Jean-Pierre Serre, eds.), Lecture Notes in Mathematics, Springer, 1973, pp. 69–190.

[Lau11] Alan G. B. Lauder, *Computations with classical and p-adic modular forms*, LMS Journal of Computation and Mathematics **14** (2011), 214–231.

[Lau14] ———, *Efficient computation of Rankin p-adic L-functions*, Computations with Modular Forms (Cham) (Gebhard Böckle and Gabor Wiese, eds.), Contributions in Mathematical and Computational Sciences, Springer International Publishing, 2014, pp. 181–200.

[Lem00] Franz Lemmermeyer, *Reciprocity Laws*, Springer Monographs in Mathematics, Springer, Berlin, Heidelberg, 2000.

[LV22] Alan Lauder and Jan Vonk, *Computing p-adic L-functions of totally real fields*, Mathematics of Computation **91** (2022), no. 334, 921–942.

[NS13] J. Neukirch and N. Schappacher, *Algebraic Number Theory*, Grundlehren Der Mathematischen Wissenschaften, Springer Berlin Heidelberg, 2013.

[PRS11] Cristian Popescu, Karl Rubin, and Alice Silverberg (eds.), *Arithmetic of L-functions*, IAS/Park City Mathematics Series, no. v. 18, American Mathematical Society ; Institute for Advanced Study, Providence, R.I. : [Princeton, N.J.], 2011.

[Rob97] Xavier-François Roblot, *Algorithmes de factorisation dans les extensions relatives et applications de la conjecture de Stark à la construction des corps de classes de rayon*, Ph.D. thesis, Bordeaux 1, 1997.

[Ser77] Jean-Pierre Serre, *Linear representations of finite groups*, vol. 42, Springer, 1977.

[Sil09] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer New York, 2009.

[Sta80] Harold M Stark, *L-functions at* $s = 1$. *IV. First derivatives at* $s = 0$, Advances in Mathematics **35** (1980), no. 3, 197–235.

[Tat81] John Tate, *On Stark's conjectures on the behavior of* $L(s, \chi)$ *at* $s = 0$, Journal of the Faculty of Science, the University of Tokyo. Sect. 1 A, Mathematics **28** (1981), no. 3, 963–978.

[The22] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.5)*, 2022.

[TY13] Brett A. Tangedal and Paul T. Young, *Explicit Computation of Gross–Stark Units over Real Quadratic Fields*, Journal of Number Theory **133** (2013), no. 3, 1045–1061.

[Von15] Jan Vonk, *Computing overconvergent forms for small primes*, LMS Journal of Computation and Mathematics **18** (2015), no. 1, 250–257.

[Zag81] Don Bernard Zagier, *Zetafunktionen und quadratische Körper*, Springer, Berlin, Heidelberg, 1981.

Mathematical Institute, University of Oxford, Woodstock Road, OX2 6GG, United Kingdom

Email address: havard.damm-johnsen@maths.ox.ac.uk