COMPOSITIO MATHEMATICA

Refined class number formulas and Kolyvagin systems

Barry Mazur and Karl Rubin

Compositio Math. **147** (2011), 56–74.

doi:10.1112/S0010437X1000494X

FOUNDATION
COMPOSITIO
MATHEMATICA

*The London
Mathematical
Society*

Compositio Math. 147 (2011) 56–74
doi:10.1112/S0010437X1000494X

Refined class number formulas and Kolyvagin systems

Barry Mazur and Karl Rubin

Abstract

We use the theory of Kolyvagin systems to prove (most of) a refined class number formula conjectured by Darmon. We show that, for every odd prime p, each side of Darmon's conjectured formula (indexed by positive integers n) is 'almost' a p-adic Kolyvagin system as n varies. Using the fact that the space of Kolyvagin systems is free of rank one over $\mathbb{Z}_p$, we show that Darmon's formula for arbitrary n follows from the case $n = 1$, which in turn follows from classical formulas.

1. Introduction

In this paper we use the theory of Kolyvagin systems to prove (most of) a conjecture of Darmon from [Dar95].

In [Gro88, Conjecture 4.1], inspired by work of the first author and Tate [MT87], and of Hayes [Hay88], Gross conjectured a 'refined class number formula' for abelian extensions K/k of global fields. Attached to this extension (and some chosen auxiliary data) there is a generalized Stickelberger element $\theta_{K/k} \in \mathbb{Z}[G]$, where $G := \mathrm{Gal}(K/k)$, with the property that, for every complex-valued character χ of G, $\chi(\theta_{K/k})$ is essentially the L-value $L(0, \chi)$ (modified by the chosen auxiliary data). Gross' conjectural formula is a congruence for $\theta_{K/k}$, modulo a certain specified power of the augmentation ideal of $\mathbb{Z}[G]$, in terms of a regulator that Gross defined.

In a very special case, Darmon formulated an analogue of Gross' conjecture involving first derivatives of L-functions at $s = 0$. Suppose F is a real quadratic field, and $K_n := F(\boldsymbol{\mu}_n)$ is the extension of F generated by nth roots of unity, with n prime to the conductor of $F/\mathbb{Q}$. Darmon defined a Stickelberger-type element $\theta'_n \in K_n^\times \otimes \mathbb{Z}[\mathrm{Gal}(K_n/F)]$, interpolating the first derivatives $L'(0, \chi\omega_F)$, where ω_F is the quadratic character attached to $F/\mathbb{Q}$ and χ runs through even Dirichlet characters of conductor n. Darmon conjectured that θ'_n is congruent, modulo a specified power of the augmentation ideal, to a regulator that he defined. See § 3 and Conjecture 3.8 below for a precise statement.

Our main result is a proof of Darmon's conjecture 'away from the 2-part'. In other words, we prove that the difference of the two sides of Darmon's conjectured congruence is an element of 2-power order.

The idea of our proof is a simple application of the results proven in [MR04a]. For every odd prime p we show that although neither the left-hand side nor the right-hand side of Darmon's conjectured congruence (as n varies) is a 'Kolyvagin system' as defined in [MR04a], each side

Received 23 September 2009, accepted in final form 31 March 2010, published online 17 August 2010.
2000 Mathematics Subject Classification 11R42 (primary), 11R27, 11R29, 11R37 (secondary).
This material is based upon work supported by the National Science Foundation under grants DMS-0700580 and DMS-0757807.

is *almost* a Kolyvagin system; moreover, both sides fail to be Kolyvagin systems in precisely the same way. That is, we show that the left-hand side and right-hand side form what we call in this paper *pre-Kolyvagin systems* in the sense that they each satisfy the specific set of local and global compatibility relations given in Definition 6.2 below. It seems that pre-Kolyvagin systems are what tend to occur 'in nature', while Kolyvagin systems satisfy a cleaner set of axioms. We show that the two concepts are equivalent, by constructing (see Proposition 6.5) a natural transformation $\mathcal{T}$ that turns pre-Kolyvagin systems into Kolyvagin systems and has the properties that:

- $\mathcal{T}$ does not change the term associated to $n = 1$; and
- $\mathcal{T}$ is an isomorphism from the $\mathbb{Z}_p$-module of pre-Kolyvagin systems to the $\mathbb{Z}_p$-module of Kolyvagin systems.

Since it was proved in [MR04a] that (in this situation) the space of Kolyvagin systems is a free $\mathbb{Z}_p$-module of rank one, it follows that if two pre-Kolyvagin systems agree when $n = 1$, then they agree for every n. In the case $n = 1$, Darmon's congruence follows from classical formulas for $L'(0, \omega_F)$, so we deduce that (the p-part, for every odd prime p of) Darmon's conjectured congruence formula holds for all n.

Darmon's conjecture begs for a generalization. A naive generalization, even just to the case where F is a real abelian extension of $\mathbb{Q}$, is unsuccessful because the definition of Darmon's regulator does not extend to the case where $[F : \mathbb{Q}] > 2$. In a forthcoming paper we will use the ideas and conjectures of [Rub96] to show how both Gross' and Darmon's conjectures are special cases of a much more general conjecture. In the current paper we treat only Darmon's conjecture because it can be presented and proved in a very concrete and explicit manner.

The paper is organized as follows. In § 2 we describe our setting and notation, and in § 3 we state Darmon's conjecture and our main result (Theorem 3.9). In § 4 we recall some work of Hales [Hal85] on quotients of powers of augmentation ideals, that will enable us to translate the definition of Kolyvagin system given in [MR04a] into a form that will be more useful for our purposes here. In § 5 we give the definition of a Kolyvagin system (for the Galois representation $\mathbb{Z}_p(1) \otimes \omega_F$). In § 6 we define pre-Kolyvagin system, and give an isomorphism between the space of pre-Kolyvagin systems and the space of Kolyvagin systems. In § 7 (respectively, § 8) we show that the 'Stickelberger' side (respectively, regulator side) of Darmon's formula is a pre-Kolyvagin system as n varies. Finally, in § 9 we combine the results of the previous sections to prove Theorem 3.9.

2. Setting and notation

Fix once and for all a real quadratic field F, and let f be the conductor of $F/\mathbb{Q}$. Let $\omega = \omega_F$ be the quadratic Dirichlet character associated to $F/\mathbb{Q}$, and τ the non-trivial element of $\mathrm{Gal}(F/\mathbb{Q})$. If M is a $\mathrm{Gal}(F/\mathbb{Q})$-module, we let M^- be the subgroup of elements of M on which τ acts as -1.

Throughout this paper ℓ will always denote a prime number. Let $\mathcal{N}$ denote the set of squarefree positive integers prime to f. If $n \in \mathcal{N}$ let n_+ be the product of all primes dividing n that split in $F/\mathbb{Q}$, and $r(n) \in \mathbb{Z}_{\geqslant 0}$ the number of prime divisors of n_+:

$$n_+ := \prod_{\ell | n, \omega(\ell) = 1} \ell,$$

$$r(n) := \#\{\ell : \ell | n_+\} = \#\{\ell : \ell | n \text{ and } \ell \text{ splits in } F\}.$$

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

For every $n \in \mathcal{N}$ let $\boldsymbol{\mu}_n$ be the Galois module of nth roots of unity in $\bar{\mathbb{Q}}$, define

$$\Gamma_n := \mathrm{Gal}(F(\boldsymbol{\mu}_n)/F) \cong \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times,$$

and let I_n denote the augmentation ideal of $\mathbb{Z}[\Gamma_n]$, which is generated over $\mathbb{Z}$ by $\{\gamma - 1 : \gamma \in \Gamma_n\}$. There is a natural isomorphism

$$\Gamma_n \cong I_n/I_n^2 \tag{1}$$

defined by sending $\gamma \in \Gamma_n$ to $\gamma - 1 \pmod{I_n^2}$. If $m|n$ then we can view Γ_m either as the quotient $\mathrm{Gal}(F(\boldsymbol{\mu}_m)/F)$ of Γ_n, or as the subgroup $\mathrm{Gal}(F(\boldsymbol{\mu}_n)/F(\boldsymbol{\mu}_{n/m}))$. With the latter identification we have

$$\Gamma_n = \prod_{\ell|n} \Gamma_\ell, \quad I_n/I_n^2 = \bigoplus_{\ell|n} I_\ell/I_\ell^2,$$

where the product and the sum are taken over primes ℓ dividing n.

We will usually write the group operation in multiplicative groups such as $F^\times$ with standard multiplicative notation (for example, with identity element 1). However, when dealing with 'mixed' groups such as $F^\times \otimes I_n^r/I_n^{r+1}$, we will write the operation additively and use 0 for the identity element.

Fix an embedding $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$.

3. Statement of the conjecture

In this section we state our modified version of Darmon's conjecture (mostly following [Dar95]) and our main result (Theorem 3.9).

If $n \in \mathcal{N}$, let $\zeta_n \in \boldsymbol{\mu}_n$ be the inverse image of $e^{2\pi i/n}$ under the chosen embedding $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$, and define the cyclotomic unit

$$\alpha_n := \prod_{\gamma \in \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_{nf})/\mathbb{Q}(\boldsymbol{\mu}_n))} \gamma(\zeta_{nf} - 1)^{\omega_F(\gamma)} \in F(\boldsymbol{\mu}_n)^\times$$

and the 'first derivative θ-element'

$$\theta_n' = \sum_{\gamma \in \Gamma_n} \gamma(\alpha_n) \otimes \gamma \in F(\boldsymbol{\mu}_n)^\times \otimes \mathbb{Z}[\Gamma_n].$$

Remark 3.1. The element θ_n' is an 'L-function derivative evaluator' in the sense that, for every even character $\chi : \Gamma_n \to \mathbb{C}^\times$, classical formulas (see, for example, [Sta80, § 2]) give

$$(\log|\cdot| \otimes \chi)(\theta_n') := \sum_{\gamma \in \Gamma_n} \chi(\gamma) \log|\gamma(\alpha_n)| = -2L_n'(0, \omega_F\chi),$$

where $L_n(s, \omega_F\chi)$ is the Dirichlet L-function with Euler factors at primes dividing n removed, and $|\cdot|$ is the absolute value corresponding to our chosen embedding $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$.

Suppose $n \in \mathcal{N}$. Let X_n be the group of divisors of F supported above $n\infty$, and let $\mathcal{E}_n := \mathcal{O}_F[1/n]^\times$, the group of n-units of F. We will write the action of $\mathbb{Z}[\Gamma_n]$ on $\mathcal{E}_n$ additively, so in particular $(1-\tau)\mathcal{E}_n = \{\epsilon/\epsilon^\tau : \epsilon \in \mathcal{E}_n\}$.

Let $\lambda_0 \in X_n$ be the archimedean place of F corresponding to our chosen embedding $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$.

Lemma 3.2. *Suppose $n \in \mathcal{N}$, and let $r = r(n)$.*

(i) *We have $X_n^- = X_{n_+}^-$, $\mathcal{E}_n^- = \mathcal{E}_{n_+}^-$, and $(1-\tau)\mathcal{E}_n = (1-\tau)\mathcal{E}_{n_+}$.*

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

(ii) *The group* $(1-\tau)\mathcal{E}_n$ *is a free abelian group of rank* $r+1$, *and is a subgroup of finite index in* $\mathcal{E}_n^-$.

(iii) *The group* X_n^- *is a free abelian group of rank* $r+1$. *If* $n_+ = \prod_{i=1}^r \ell_i$, *and* $\ell_i = \lambda_i\lambda_i^\tau$, *then* $\{\lambda_0 - \lambda_0^\tau, \lambda_1 - \lambda_1^\tau, \dots, \lambda_r - \lambda_r^\tau, \}$ *is a basis of* X_n^-.

Proof. The only part that is not clear is that $(1-\tau)\mathcal{E}_n$ is torsion-free, i.e. $-1 \notin (1-\tau)\mathcal{E}_n$. Let $d>1$ be a squarefree integer such that $F=\mathbb{Q}(\sqrt{d})$. If $x^\tau = -x$, then $x/\sqrt{d} \in \mathbb{Q}$, so x is not a unit at the primes dividing d. Since n is prime to d, we cannot have $x \in \mathcal{E}_n$. □

Definition 3.3. A *standard* $\mathbb{Z}$-basis of X_n^- is a basis of the form described in Lemma 3.2(iii). Given a standard basis of X_n^-, a $\mathbb{Z}$-basis $\{\epsilon_0, \dots, \epsilon_r\}$ of $(1-\tau)\mathcal{E}_n$ will be said to be *oriented* if the (regulator) determinant of the logarithmic embedding

$$(1-\tau)\mathcal{E}_n \longrightarrow X_n^- \otimes \mathbb{R}, \quad \epsilon \mapsto \sum_{\lambda | n_+ \infty} \log |\epsilon|_\lambda \cdot \lambda$$

with respect to the two bases is positive. Concretely, this regulator is the determinant of the matrix whose entry in row i and column j is $\log |\epsilon_j|_{\lambda_i}$.

Remark 3.4. Choosing a standard basis of X_n^- is equivalent to ordering the prime divisors ℓ_i of n_+ and choosing one prime of F above each ℓ_i.

Any basis of $(1-\tau)\mathcal{E}_n$ can be oriented either by reordering the basis, or inverting one of the basis elements.

Definition 3.5. Suppose $n \in \mathcal{N}$ and λ is a prime of F dividing n_+. Define a homomorphism

$$[\,\cdot\,]_\lambda^n : F^\times \longrightarrow I_n/I_n^2$$

by

$$[x]_\lambda^n = [x, F_\lambda(\boldsymbol{\mu}_n)/F_\lambda] - 1 \pmod{I_n^2}$$

where $[x, F_\lambda(\boldsymbol{\mu}_n)/F_\lambda] \in \Gamma_n$ is the local Artin symbol.

Note that if $\mathrm{ord}_\lambda(x) = 0$, then $[x, F_\lambda(\boldsymbol{\mu}_n)/F_\lambda]$ belongs to the inertia group $\Gamma_\ell \subset \Gamma_n$, so $[x]_\lambda^n = [x]_\lambda^\ell \in I_\ell/I_\ell^2$ and $[x]_\lambda^{n/\ell} = 0$. In general, if $d|n$ then

$$[x]_\lambda^n = [x]_\lambda^d + [x]_\lambda^{n/d} \in I_d/I_d^2 \oplus I_{n/d}/I_{n/d}^2 = I_n/I_n^2.$$

Definition 3.6 (See [Dar95, p. 308]). Suppose $n \in \mathcal{N}$, and let $r = r(n)$. Choose a standard basis $\{\lambda_0 - \lambda_0^\tau, \dots, \lambda_r - \lambda_r^\tau\}$ of X_n^- and an oriented basis $\{\epsilon_0, \dots, \epsilon_r\}$ of $(1-\tau)\mathcal{E}_n$, and define the regulator $R_n \in \mathcal{E}_n^- \otimes I_n^r/I_n^{r+1}$ by

$$R_n := \begin{vmatrix} \epsilon_0 & \epsilon_1 & \cdots & \epsilon_r \\ [\epsilon_0]_{\lambda_1}^n & [\epsilon_1]_{\lambda_1}^n & \cdots & [\epsilon_r]_{\lambda_1}^n \\ \vdots & \vdots & & \vdots \\ [\epsilon_0]_{\lambda_r}^n & [\epsilon_1]_{\lambda_r}^n & \cdots & [\epsilon_r]_{\lambda_r}^n \end{vmatrix} \in (1-\tau)\mathcal{E}_n \otimes I_n^r/I_n^{r+1}.$$

This determinant, and the ones that follow below, are meant to be evaluated by expanding by minors along the top row, i.e.

$$R_n := \sum_{j=0}^{r} (-1)^j \epsilon_j \otimes \det(A_{1j}), \tag{2}$$

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

where A_{1j} is the $r \times r$ matrix (with entries in I_n/I_n^2) obtained by removing the first row and jth column of the matrix above.

Note that this definition of R_n does not depend on the choice of $\mathbb{Z}$-bases. The possible ambiguity of ± 1 is removed by requiring that the basis of $(1-\tau)\mathcal{E}_n$ be oriented.

Let h_n denote the 'n-class number' of F, i.e. the order of the ideal class group $\mathrm{Pic}(\mathcal{O}_F[1/n])$. For the rest of this section we write simply r instead of $r(n)$ for the number of prime factors of n_+.

Theorem 3.7 (Darmon [Dar95, Theorem 4.2]). *For every $n \in \mathcal{N}$, we have*

$$\theta'_n \in F(\boldsymbol{\mu}_n)^\times \otimes I_n^r.$$

For $n \in \mathcal{N}$, let $\tilde{\theta}'_n$ denote the image of θ'_n in $F(\boldsymbol{\mu}_n)^\times \otimes I_n^r/I_n^{r+1}$. Let s be the number of prime divisors of n/n_+. The following is a slightly modified (see Remark 3.11(i) below) version of Darmon's 'leading term' conjecture [Dar95, Conjecture 4.3].

Conjecture 3.8. For every $n \in \mathcal{N}$, we have

$$\tilde{\theta}'_n = -2^s h_n R_n \quad \text{in } (F(\boldsymbol{\mu}_n)^\times/\{\pm 1\}) \otimes I_n^r/I_n^{r+1}.$$

The main theorem of this paper is the following.

Theorem 3.9. *For every $n \in \mathcal{N}$, we have*

$$\tilde{\theta}'_n = -2^s h_n R_n \quad \text{in } F(\boldsymbol{\mu}_n)^\times \otimes I_n^r/I_n^{r+1} \otimes \mathbb{Z}[1/2].$$

In other words, the p-part of Conjecture 3.8 holds for every odd prime p; in still other words, $\tilde{\theta}'_n + 2^s h_n R_n$ has 2-power order in $F(\boldsymbol{\mu}_n)^\times \otimes I_n^r/I_n^{r+1}$.

A key step in the proof of Theorem 3.9 is the following observation.

Proposition 3.10 (Darmon [Dar95, Theorem 4.5(1)]). *Conjecture 3.8 holds if $n = 1$.*

Proof. When $n = 1$ we have $r = 0$, $I_n^r/I_n^{r+1} = \mathbb{Z}$, $\tilde{\theta}'_1 = \theta'_1 = \alpha_1 \in \mathcal{O}_F^\times$, and $R_1 = \epsilon/\epsilon^\tau$, where ϵ is a generator of $\mathcal{O}_F^\times/\{\pm 1\}$ and $|\epsilon/\epsilon^\tau| = |\epsilon|^2 > 1$ at our specified archimedean place. Dirichlet's analytic class number formula shows that

$$-\tfrac{1}{2}\log|\alpha_1| = L'(0,\omega_F) = h_F \log|\epsilon| = \tfrac{1}{2} h_F \log|\epsilon/\epsilon^\tau|,$$

where $h_F = h_1$ is the class number of F. Hence $\alpha_1 = \pm(\epsilon/\epsilon^\tau)^{-h_F}$ in $\mathcal{O}_F^\times$. □

Remarks 3.11.

(i) In Darmon's formulation [Dar95, Conjecture 4.3], the regulator R_n was defined with respect to a basis of $\mathcal{E}_n^-/\{\pm 1\}$ instead of $(1-\tau)\mathcal{E}_n$, and there was an extra factor of 2 on the right-hand side. This agrees with Conjecture 3.8 if and only if $[\mathcal{E}_n^- : \pm(1-\tau)\mathcal{E}_n] = 2$, i.e. if and only if $-1 \notin \mathbb{N}_{F/\mathbb{Q}}\mathcal{E}_n$.

(ii) The ambiguity of ± 1 in Conjecture 3.8 is necessary. Namely, even when $n = 1$, we may only have $\tilde{\theta}'_1 = h_1 R_1$ in $\mathcal{O}_F^\times/\{\pm 1\}$. Since α_1 is always positive (it is a norm from a CM field to F), the proof of Proposition 3.10 shows that $\tilde{\theta}'_1 \neq -h_1 R_1$ in $F^\times$ when h_F is odd and $\mathcal{O}_F^\times$ has a unit of norm -1. Note that in this case $\tilde{\theta}'_1$ and $-h_1 R_1$ differ (multiplicatively) by an element of order 2 in $F^\times$, so the discrepancy disappears when we tensor with $\mathbb{Z}[1/2]$.

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

4. Augmentation quotients

Definition 4.1. Suppose $n \in \mathcal{N}$, and let $r = r(n)$. Let $\mathcal{I}_n^{\mathrm{new}} \subset I_n^r/I_n^{r+1}$ be the (cyclic) subgroup generated by monomials $\prod_{\ell|n_+}(\gamma_\ell - 1)$ with $\gamma_\ell \in \Gamma_\ell$. Let $\mathcal{I}_n^{\mathrm{old}} \subset I_n^r/I_n^{r+1}$ be the subgroup generated by monomials $\prod_{i=1}^r(\gamma_i - 1)$ where each $\gamma_i \in \Gamma_{\ell_i}$ for some ℓ_i dividing n, and $\{\ell_1, \dots, \ell_r\} \neq \{\ell : \ell|n_+\}$ (i.e. either one of the ℓ_i divides n/n_+, or $\ell_i = \ell_j$ for some $i \neq j$). If $n = d_1 d_2$ then there is a natural identification $\mathcal{I}_n^{\mathrm{new}} = \mathcal{I}_{d_1}^{\mathrm{new}}\mathcal{I}_{d_2}^{\mathrm{new}} \subset I_n^r/I_n^{r+1}$, and if $n = \ell$ is prime then $\mathcal{I}_\ell^{\mathrm{new}} = I_\ell/I_\ell^2$ and $\mathcal{I}_\ell^{\mathrm{old}} = 0$.

If $d|n$, let

$$\pi_d : \mathbb{Z}[\Gamma_n] \twoheadrightarrow \mathbb{Z}[\Gamma_d] \hookrightarrow \mathbb{Z}[\Gamma_n]$$

denote the composition of the natural maps. We also write π_d for the induced map on I_n^k/I_n^{k+1} for $k \geqslant 0$.

The following proposition is based on work of Hales [Hal85].

Proposition 4.2. *Suppose $n \in \mathcal{N}$, and $r = r(n)$. Then:*

(i) $I_n^r/I_n^{r+1} = \mathcal{I}_n^{\mathrm{new}} \oplus \mathcal{I}_n^{\mathrm{old}}$;
(ii) *if $d|n_+$ and $d > 1$, then $\pi_{n/d}(\mathcal{I}_n^{\mathrm{new}}) = 0$ and $\pi_{n/d}(I_n^r/I_n^{r+1}) \subset \mathcal{I}_n^{\mathrm{old}}$;*
(iii) $\mathcal{I}_n^{\mathrm{new}} = \{v \in I_n^r/I_n^{r+1} : \pi_{n/\ell}(v) = 0$ *for every ℓ dividing n_+*$\}$;
(iv) *the map $\otimes_{\ell|n_+}\Gamma_\ell \to \mathcal{I}_n^{\mathrm{new}}$ defined by $\otimes_{\ell|n_+}\gamma_\ell \mapsto \prod_{\ell|n_+}(\gamma_\ell - 1)$ is an isomorphism.*

Proof. Let A_n be the polynomial ring $\mathbb{Z}[Y_\ell : \ell|n]$ with one variable Y_ℓ for each prime ℓ dividing n. Fix a generator σ_ℓ of Γ_ℓ for every ℓ dividing n, and define a map $A_n \to \mathbb{Z}[\Gamma_n]$ by sending $Y_\ell \mapsto \sigma_\ell - 1$. By Corollary 2 of [Hal85], this map induces an isomorphism from the homogeneous degree-r part of $A_n/(J_n + J_n')$ to I_n^r/I_n^{r+1}, where J_n is the ideal of A_n generated by $\{(\ell - 1)Y_\ell : \ell|n\}$, and J_n' is the ideal generated by certain other explicit homogeneous relations (see [Hal85, Lemma 2]). The only fact we need about these 'extra' relations is:

if $f \in J_n'$, then every monomial that occurs in f is divisible by the square of some Y_ℓ. (3)

Note that $\mathcal{I}_n^{\mathrm{new}}$ is the image in I_n^r/I_n^{r+1} of the subgroup of $A_n/(J_n + J_n')$ generated by $\mathbf{Y}_n$, where $\mathbf{Y}_n := \prod_{\ell|n_+} Y_\ell$. Similarly, $\mathcal{I}_n^{\mathrm{old}}$ is the image of the subgroup generated by all other monomials of degree r. By (3), $\mathbf{Y}_n$ does not occur in any of the relations in J_n', and assertion (i) follows.

Assertion (ii) is clear, since $\pi_{n/d}$ kills those monomials that include $(\gamma - 1)$ with $\gamma \in \Gamma_\ell$ for ℓ dividing d, and leaves the other monomials unchanged.

Fix $v \in I_n^r/I_n^{r+1}$. If $v \in \mathcal{I}_n^{\mathrm{new}}$ and $\ell|n_+$, then $\pi_{n/\ell}(v) = 0$ by (ii). Conversely, suppose that $\pi_{n/\ell}(v) = 0$ for every ℓ dividing n_+. Choose $f \in A_n$ to be homogeneous of degree r representing v, and suppose f has the minimum number of monomials among all representatives of v. We will show that $\mathbf{Y}_n|f$, and hence $v \in \mathcal{I}_n^{\mathrm{new}}$.

Fix a prime ℓ dividing n_+. The map $\pi_{n/\ell} : \mathbb{Z}[\Gamma_n] \twoheadrightarrow \mathbb{Z}[\Gamma_{n/\ell}] \hookrightarrow \mathbb{Z}[\Gamma_n]$ corresponds to the map $A_n \to A_n$ defined by setting $Y_\ell = 0$. Since $\pi_{n/\ell}(v) = 0$, substituting $Y_\ell = 0$ in f gives a relation in $J_n + J_n'$, i.e. $f = Y_\ell \cdot g + h$ where g is homogeneous of degree $r - 1$, $h \in J_n + J_n'$, and Y_ℓ does not occur in h. But then $Y_\ell \cdot g$ represents v, so the minimality assumption on f implies that $h = 0$. Therefore $Y_\ell|f$ for every ℓ dividing n_+, so $\mathbf{Y}_n|f$ and $v \in \mathcal{I}_n^{\mathrm{new}}$. This proves (iii).

Let $g := \gcd(\{\ell - 1 : \ell|n_+\})$. Then $g\mathbf{Y}_n \in J_n$. It follows from (3) that the monomial $\mathbf{Y}_n$ only occurs in elements of $J_n + J_n'$ with coefficients divisible by g. Therefore $\mathcal{I}_n^{\mathrm{new}}$ is cyclic of order g, and so is $\otimes_{\ell|n_+}\Gamma_\ell$. Clearly the map $\otimes_{\ell|n_+}\Gamma_\ell \to \mathcal{I}_n^{\mathrm{new}}$ of (iv) is surjective, so it must be an isomorphism. □

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

If $v \in I_n^r/I_n^{r+1}$, let $\langle v\rangle_n^{\text{new}}$ denote the projection of v to $\mathcal{I}_n^{\text{new}}$ under the splitting of Proposition 4.2(i). We will use the following lemma without explicit reference in some of our computations in §§ 6 and 8. Its proof is left as an exercise.

Lemma 4.3. *Suppose $d|n$, $v \in \mathcal{I}_{n/d}^{\text{new}}$, and $w \in I_n^{r(d)}/I_n^{r(d)+1}$. Then*

$$\langle vw\rangle_n^{\text{new}} = \langle v\pi_d(w)\rangle_n^{\text{new}} = v\langle \pi_d(w)\rangle_d^{\text{new}}.$$

5. Kolyvagin systems

Fix an odd prime p. To prove Theorem 3.9 we need to introduce Kolyvagin systems, as defined in [MR04a]. (See in particular [MR04a, § 6.1], and also [MR04b], for the case of Kolyvagin systems associated to even Dirichlet characters that we use here.)

Let $\hat{F}^\times$ denote the p-adic completion of $F^\times$. Similarly, for every rational prime ℓ let $F_\ell := F \otimes \mathbb{Q}_\ell$, $\mathcal{O}_\ell := \mathcal{O}_F \otimes \mathbb{Z}_\ell$, and define $\hat{F}_\ell^\times$ and $\hat{\mathcal{O}}_\ell^\times$ to be their p-adic completions. We define the 'finite subgroup' $\hat{F}_{\ell,\mathrm{f}}^\times$ to be the 'unit part' of $\hat{F}_\ell^\times$,

$$\hat{F}_{\ell,\mathrm{f}}^\times := \hat{\mathcal{O}}_\ell^\times \subset \hat{F}_\ell^\times.$$

If $\ell = \lambda\lambda^\tau$ splits in F, define the 'transverse subgroup' $\hat{F}_{\ell,\mathrm{tr}}^\times \subset \hat{F}_\ell^\times$ to be the (closed) subgroup generated by $(\ell, 1)$ and $(1, \ell)$, where we identify $F_\ell^\times$ with $F_\lambda^\times \times F_{\lambda^\tau}^\times \cong \mathbb{Q}_\ell^\times \times \mathbb{Q}_\ell^\times$. Then we have a canonical splitting $\hat{F}_\ell^\times = \hat{F}_{\ell,\mathrm{f}}^\times \times \hat{F}_{\ell,\mathrm{tr}}^\times$, and since p is odd,

$$(\hat{F}_\ell^\times)^- = (\hat{F}_{\ell,\mathrm{f}}^\times)^- \times (\hat{F}_{\ell,\mathrm{tr}}^\times)^-. \tag{4}$$

Definition 5.1. If $\ell \neq p$ splits in F, define the *finite-singular isomorphism*

$$\phi_\ell^{\mathrm{fs}} : (\hat{F}_{\ell,\mathrm{f}}^\times)^- \xrightarrow{\sim} (\hat{F}_{\ell,\mathrm{tr}}^\times)^- \otimes I_\ell/I_\ell^2$$

by

$$\begin{aligned}\phi_\ell^{\mathrm{fs}}(x) &= (\ell, 1) \otimes ([x_\lambda, F_\lambda(\boldsymbol{\mu}_\ell)/F_\lambda] - 1) + (1, \ell) \otimes ([x_{\lambda^\tau}, F_{\lambda^\tau}(\boldsymbol{\mu}_\ell)/F_{\lambda^\tau}] - 1)\\ &= (\ell, \ell^{-1}) \otimes ([x_\lambda, F_\lambda(\boldsymbol{\mu}_\ell)/F_\lambda] - 1),\end{aligned}$$

where $x = (x_\lambda, x_{\lambda^\tau}) \in \hat{F}_\lambda^\times \times \hat{F}_{\lambda^\tau}^\times = \hat{\mathbb{Q}}_\ell^\times \times \hat{\mathbb{Q}}_\ell^\times$ with $x_{\lambda^\tau} = x_\lambda^{-1} \in \hat{\mathbb{Z}}_\ell^\times$, and $[\,\cdot\,, F_\lambda(\boldsymbol{\mu}_\ell)/F_\lambda]$ is the local Artin symbol. (Concretely, note that if $u \in \mathbb{Z}_\ell^\times$ then $[u, F_\lambda(\boldsymbol{\mu}_\ell)/F_\lambda]$ is the automorphism in Γ_ℓ that sends ζ_ℓ to $\zeta_\ell^{u^{-1}}$.) Then ϕ_ℓ^{fs} is a well-defined isomorphism (both the domain and range are free of rank one over $\mathbb{Z}_p/(\ell-1)\mathbb{Z}_p$), independent of the choice of λ versus λ^τ.

Definition 5.2. Let $\mathcal{N}_p := \{n \in \mathcal{N} : p \nmid n\}$. A *Kolyvagin system* $\boldsymbol{\kappa}$ (for the Galois representation $\mathbb{Z}_p(1) \otimes \omega_F$) is a collection

$$\{\kappa_n \in (\hat{F}^\times)^- \otimes \mathcal{I}_n^{\text{new}} : n \in \mathcal{N}_p\}$$

satisfying the following properties for every rational prime ℓ. Let $(\kappa_n)_\ell$ denote the image of κ_n in $(\hat{F}_\ell^\times)^- \otimes \mathcal{I}_n^{\text{new}}$.

(i) If $\ell \nmid n$, then $(\kappa_n)_\ell \in (\hat{F}_{\ell,\mathrm{f}}^\times)^- \otimes \mathcal{I}_n^{\text{new}}$.

(ii) If $\ell | n_+$, then $(\kappa_n)_\ell = (\phi_\ell^{\mathrm{fs}} \otimes 1)(\kappa_{n/\ell})_\ell$.

(iii) If $\ell | n/n_+$, then $\kappa_n = \kappa_{n/\ell}$.

Let $\mathbf{KS}(F)$ denote the $\mathbb{Z}_p$-module of Kolyvagin systems for $\mathbb{Z}_p(1) \otimes \omega_F$.

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

Remark 5.3. Let $\mathcal{N}_p^+ := \{n \in \mathcal{N}_p : \text{all } \ell | n \text{ split in } F/\mathbb{Q}\}$. In [MR04a], a Kolyvagin system was defined to be a collection of classes $\{\kappa_n \in (\hat{F}_\ell^\times)^- \otimes (\otimes_{\ell|n}\Gamma_\ell) : n \in \mathcal{N}_p^+\}$, and ϕ_ℓ^{fs} took values in $(\hat{F}_{\ell,\mathrm{tr}}^\times)^- \otimes \Gamma_\ell$. We use Proposition 4.2(iv) to replace $\otimes_{\ell|n_+}\Gamma_\ell$ by $\mathcal{I}_n^{\mathrm{new}}$ and (1) to replace Γ_ℓ by I_ℓ/I_ℓ^2, which will be more convenient for our purposes here. Also, a Kolyvagin system $\{\kappa_n : n \in \mathcal{N}_p^+\}$ as in [MR04a] extends uniquely to $\{\kappa_n : n \in \mathcal{N}_p\}$ simply by setting $\kappa_n := \kappa_{n_+}$ for $n \in \mathcal{N}_p - \mathcal{N}_p^+$.

The following theorem is the key to our proof of Theorem 3.9.

Theorem 5.4. *Suppose* $\boldsymbol{\kappa}, \boldsymbol{\kappa}' \in \mathbf{KS}(F)$. *If* $\kappa_1 = \kappa_1'$, *then* $\kappa_n = \kappa_n'$ *for every* $n \in \mathcal{N}_p$.

Proof. We follow [MR04a, § 6.1], with $R = \mathbb{Z}_p$, $\rho = \omega_F$, $T = \mathbb{Z}_p(1) \otimes \omega_F$, and with the Selmer structure denoted $\mathcal{F}$ in [MR04a]. By [MR04a, Lemma 6.1.5 and Proposition 6.1.6], the hypotheses needed to apply the results [MR04a, § 5.2] all hold, and the core rank of T is one.

By [MR04a, Theorem 5.2.10(ii)], $\mathbf{KS}(F)$ is a free $\mathbb{Z}_p$-module of rank one. Therefore (switching $\boldsymbol{\kappa}$ and $\boldsymbol{\kappa}'$ if necessary) there is an $a \in \mathbb{Z}_p$ such that $\boldsymbol{\kappa}' = a\boldsymbol{\kappa}$, i.e. $\kappa_n' = a\kappa_n$ for every $n \in \mathcal{N}_p$. If $\boldsymbol{\kappa}$ is identically zero, then so is $\boldsymbol{\kappa}'$ and we are done. If $\boldsymbol{\kappa}$ is not identically zero, then (since the ideal class group of F is finite) [MR04a, Theorem 5.2.12(v)] shows that $\kappa_1 \neq 0$. Since $\kappa_1' = \kappa_1$ in the torsion-free $\mathbb{Z}_p$-module $(\hat{F}^\times)^-$ (in fact property (i) above shows that $\kappa_1 \in (\mathcal{O}_F^\times \otimes \mathbb{Z}_p)^-$), we must have $a = 1$. □

6. Pre-Kolyvagin systems

Keep the fixed odd prime p. The right-hand and left-hand sides of Conjecture 3.8 are 'almost' Kolyvagin systems. If they were Kolyvagin systems, then since they agree when $n = 1$ (Proposition 3.10), they would agree for all n by Theorem 5.4, and Theorem 3.9 would be proved.

In this section we define what we call 'pre-Kolyvagin systems', and show that a pre-Kolyvagin system can be transformed into a Kolyvagin system. Using Theorem 5.4, we deduce (Corollary 6.6 below) that if two pre-Kolyvagin systems agree when $n = 1$, then they agree for every n. In §§ 7 and 8, respectively, we will show that the left-hand and right-hand sides of Conjecture 3.8 are pre-Kolyvagin systems. Then Theorem 3.9 will follow from Corollary 6.6 and Proposition 3.10.

If $x \in (\hat{F}^\times)^- \otimes I_n^r/I_n^{r+1}$, let x_ℓ denote the image of x in $(\hat{F}_\ell^\times)^- \otimes I_n^r/I_n^{r+1}$, and if $\ell \in \mathcal{N}_p$ splits in $F/\mathbb{Q}$, let $x_{\ell,\mathrm{f}} \in (\hat{F}_{\ell,\mathrm{f}}^\times)^- \otimes I_n^r/I_n^{r+1}$ and $x_{\ell,\mathrm{tr}} \in (\hat{F}_{\ell,\mathrm{tr}}^\times)^- \otimes I_n^r/I_n^{r+1}$ denote the projections of x_ℓ induced by the splitting (4). Let $\langle x \rangle_n^{\mathrm{new}} \in (\hat{F}^\times)^- \otimes \mathcal{I}_n^{\mathrm{new}}$ denote the projection of x induced by the splitting of Proposition 4.2(i), and similarly for $\langle x_\ell \rangle_n^{\mathrm{new}}$ and $\langle x_{\ell,\mathrm{f}} \rangle_n^{\mathrm{new}}$.

Definition 6.1. If $n \in \mathcal{N}$ and $d = \prod_{i=1}^t \ell_i$ divides n_+, let $M_{n,d} = (m_{ij})$ be the $t \times t$ matrix with entries in I_n/I_n^2,

$$m_{ij} = \begin{cases} \pi_{n/d}(\mathrm{Fr}_{\ell_i} - 1) & \text{if } i = j, \\ \pi_{\ell_j}(\mathrm{Fr}_{\ell_i} - 1) & \text{if } i \neq j. \end{cases}$$

We let $M_d := M_{d,d}$, where $\pi_1(\mathrm{Fr}_\ell - 1)$ is understood to be zero, so that all diagonal entries of M_d are zero. Define

$$\mathcal{D}_{n,d} := \det(M_{n,d}) \in I_n^t/I_n^{t+1}, \quad \mathcal{D}_d := \det(M_d) \in \mathcal{I}_d^{\mathrm{new}} \subset I_n^t/I_n^{t+1}.$$

By convention we let $\mathcal{D}_{n,1} = \mathcal{D}_1 = 1$. Note that $\mathcal{D}_{n,d}$ and $\mathcal{D}_d$ are independent of the ordering of the prime factors of d.

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

Definition 6.2. A *pre-Kolyvagin system* $\boldsymbol{\kappa}$ (for $\mathbb{Z}_p(1)\otimes\omega_F$) is a collection

$$\{\kappa_n \in (\hat{F}^\times)^- \otimes I_n^r/I_n^{r+1} : n\in\mathcal{N}_p\}$$

where $r=r(n)$, satisfying the following properties for every rational prime ℓ.

(i) If $\ell\nmid n$, then $(\kappa_n)_\ell \in (\hat{F}^\times_{\ell,\mathrm{f}})^- \otimes I_n^r/I_n^{r+1}$.
(ii) If $\ell|n_+$, then $(1\otimes\pi_{n/\ell})\kappa_n = \kappa_{n/\ell}\,\pi_{n/\ell}(1-\mathrm{Fr}_\ell)$.
(iii) If $\ell|n_+$, then $\langle(\kappa_n)_{\ell,\mathrm{tr}}\rangle_n^{\mathrm{new}} = (\phi_\ell^{\mathrm{fs}}\otimes 1)(\langle(\kappa_{n/\ell})_\ell\rangle_{n/\ell}^{\mathrm{new}})$.
(iv) If $\ell|n_+$, then $\sum_{d|n_+}\langle(\kappa_{n/d})_{\ell,\mathrm{f}}\rangle_{n/d}^{\mathrm{new}}\,\mathcal{D}_d = 0$.
(v) If $\ell|n/n_+$, then $\langle\kappa_n\rangle_n^{\mathrm{new}} = \langle\kappa_{n/\ell}\rangle_{n/\ell}^{\mathrm{new}}$.

Let $\mathbf{PKS}(F)$ denote the $\mathbb{Z}_p$-module of pre-Kolyvagin systems for $\mathbb{Z}_p(1)\otimes\omega_F$.

Definition 6.3. If $\boldsymbol{\kappa}=\{\kappa_n : n\in\mathcal{N}_p\}$ is a pre-Kolyvagin system, define $\tilde{\boldsymbol{\kappa}}=\{\tilde{\kappa}_n : n\in\mathcal{N}_p\}$ by

$$\tilde{\kappa}_n := \sum_{d|n_+}\kappa_{n/d}\mathcal{D}_{n,d}.$$

Lemma 6.4. *Suppose $n\in\mathcal{N}_p$ and $d|n$.*

(i) *If $\ell|d$, then $\pi_{n/\ell}(\mathcal{D}_{n,d}) = \pi_{n/d}(\mathrm{Fr}_\ell-1)\mathcal{D}_{n/\ell,d/\ell}$.*
(ii) *If $\ell\nmid d$, then $\pi_{n/\ell}(\mathcal{D}_{n,d}) = \mathcal{D}_{n/\ell,d}$.*
(iii) $\pi_d(\mathcal{D}_{n,d}) = \mathcal{D}_d \in \mathcal{I}_d^{\mathrm{new}}$.

Proof. Suppose $\ell|d$. The column of $\pi_{n/\ell}(M_{n,d})$ corresponding to ℓ consists of all zeros except for $\pi_{n/d}(\mathrm{Fr}_\ell-1)$ on the diagonal. The first assertion follows from this, and (ii) and (iii) follow directly from the definition. □

Proposition 6.5. *The map $\boldsymbol{\kappa}\mapsto\tilde{\boldsymbol{\kappa}}$ of Definition 6.3 is a $\mathbb{Z}_p$-module isomorphism $\mathbf{PKS}(F)\xrightarrow{\sim}\mathbf{KS}(F)$ between free $\mathbb{Z}_p$-modules of rank one.*

Proof. The $\mathbb{Z}_p$-linearity is clear. The injectivity is clear as well, since it follows easily by induction that if $\tilde{\kappa}_n=0$ for all n, then $\kappa_n=0$ for all n.

We next show that if $\boldsymbol{\kappa}$ is a pre-Kolyvagin system, then $\tilde{\boldsymbol{\kappa}}$ is a Kolyvagin system. In other words, we need to show for every $n\in\mathcal{N}_p$ that:

(a) $\tilde{\kappa}_n \in (\hat{F}^\times)^-\otimes\mathcal{I}_n^{\mathrm{new}}$;
(b) if $\ell\nmid n$, then $(\tilde{\kappa}_n)_\ell \in (\hat{F}^\times_{\ell,\mathrm{f}})^-\otimes\mathcal{I}_n^{\mathrm{new}}$;
(c) if $\ell|n_+$, then $(\tilde{\kappa}_n)_{\ell,\mathrm{tr}} = (\phi_\ell^{\mathrm{fs}}\otimes 1)((\kappa_{n/\ell})_\ell)$;
(d) if $\ell|n_+$, then $(\tilde{\kappa}_n)_{\ell,\mathrm{f}}=0$;
(e) if $\ell|n/n_+$, then $\tilde{\kappa}_n=\tilde{\kappa}_{n/\ell}$.

Fix $n\in\mathcal{N}_p$, and suppose that $\ell|n_+$. Then

$$\begin{aligned}(1\otimes\pi_{n/\ell})(\tilde{\kappa}_n) &= \sum_{d|n_+,\ell\nmid d}(1\otimes\pi_{n/\ell})(\kappa_{n/d}\mathcal{D}_{n,d}) + \sum_{d|n_+,\ell|d}(1\otimes\pi_{n/\ell})(\kappa_{n/d}\mathcal{D}_{n,d})\\ &= \sum_{d|(n_+/\ell)}\kappa_{n/(d\ell)}\,\pi_{n/\ell}(\mathcal{D}_{n,d\ell}) + (1\otimes\pi_{n/(d\ell)})(\kappa_{n/d})\pi_{n/\ell}(\mathcal{D}_{n,d}).\end{aligned}$$

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

Fix a divisor d of n_+/ℓ. By Lemma 6.4(i),

$$\kappa_{n/(d\ell)}\ \pi_{n/\ell}(\mathcal{D}_{n,d\ell}) = \kappa_{n/(d\ell)}\ \pi_{n/(d\ell)}(\mathrm{Fr}_\ell - 1)\mathcal{D}_{n/\ell,d}.$$

Also, $(1\otimes\pi_{n/(d\ell)})(\kappa_{n/d}) = \kappa_{n/(d\ell)}\ \pi_{n/(d\ell)}(1-\mathrm{Fr}_\ell)$ by Definition 6.2(ii), so by Lemma 6.4(ii)

$$(1\otimes\ \pi_{n/(d\ell)})(\kappa_{n/d})\pi_{n/\ell}(\mathcal{D}_{n,d}) = \kappa_{n/(d\ell)}\ \pi_{n/(d\ell)}(1-\mathrm{Fr}_\ell)\mathcal{D}_{n/\ell,d}.$$

Thus $(1\otimes\pi_{n/\ell})(\tilde\kappa_n)=0$ for every ℓ dividing n. Since $(\hat F^\times)^-$ is a free $\mathbb{Z}_p$-module, it follows from Proposition 4.2(iii) that $\tilde\kappa_n\in(\hat F^\times)^-\otimes\mathcal{I}_n^{\mathrm{new}}$. This is property (a) above.

By property (a), and using the fact that $\pi_d(\mathcal{D}_{n,d})\in\mathcal{I}_d^{\mathrm{new}}$, we have

$$\tilde\kappa_n = \langle\tilde\kappa_n\rangle_n^{\mathrm{new}} = \sum_{d|n_+}\langle\kappa_{n/d}\rangle_{n/d}^{\mathrm{new}}\ \pi_d(\mathcal{D}_{n,d}).$$

If $\ell\nmid n$, then Definition 6.2(i) of a pre-Kolyvagin system shows that $\langle(\kappa_{n,d})_\ell\rangle_{n/d}^{\mathrm{new}}\in(\hat F_{\ell,\mathrm{f}}^\times)^-\otimes\mathcal{I}_{n/d}^{\mathrm{new}}$ for every d, so $(\tilde\kappa_n)_\ell\in(\hat F_{\ell,\mathrm{f}}^\times)^-\otimes\mathcal{I}_n^{\mathrm{new}}$. This is property (b).

Now suppose $\ell|n_+$. For property (c), using Definition 6.2(i) we have

$$(\tilde\kappa_n)_{\ell,\mathrm{tr}} = \sum_{d|n_+}(\kappa_{n/d})_{\ell,\mathrm{tr}}\mathcal{D}_{n,d} = \sum_{d|(n_+/\ell)}(\kappa_{n/d})_{\ell,\mathrm{tr}}\mathcal{D}_{n,d}.$$

Projecting into $\mathcal{I}_n^{\mathrm{new}}$, and using property (a), Definition 6.2(ii), and Lemma 6.4(ii), we have

$$\begin{aligned}
(\tilde\kappa_n)_{\ell,\mathrm{tr}} &= \langle(\tilde\kappa_n)_{\ell,\mathrm{tr}}\rangle_n^{\mathrm{new}} = \sum_{d|(n_+/\ell)}\langle(\kappa_{n/d})_{\ell,\mathrm{tr}}\mathcal{D}_{n,d}\rangle_n^{\mathrm{new}}\\
&= \sum_{d|(n_+/\ell)}\langle(\phi_\ell^{\mathrm{fs}}\otimes 1)((\kappa_{n/(d\ell)})_\ell)\ \pi_{n/\ell}(\mathcal{D}_{n,d})\rangle_n^{\mathrm{new}}\\
&= \sum_{d|(n_+/\ell)}\langle(\phi_\ell^{\mathrm{fs}}\otimes 1)((\kappa_{n/(d\ell)})_\ell)\mathcal{D}_{n/\ell,d}\rangle_n^{\mathrm{new}}\\
&= \langle(\phi_\ell^{\mathrm{fs}}\otimes 1)(\tilde\kappa_{n/\ell})\rangle_n^{\mathrm{new}} = (\phi_\ell^{\mathrm{fs}}\otimes 1)(\langle\tilde\kappa_{n/\ell}\rangle_{n/\ell}^{\mathrm{new}}) = (\phi_\ell^{\mathrm{fs}}\otimes 1)(\tilde\kappa_{n/\ell}).
\end{aligned}$$

This is property (c). For property (d), using property (a), Lemma 6.4(iii), and Definition 6.2(iv) we have

$$(\tilde\kappa_n)_{\ell,\mathrm{f}} = \langle(\tilde\kappa_n)_{\ell,\mathrm{f}}\rangle_n^{\mathrm{new}} = \sum_{d|n_+}\langle(\kappa_{n/d})_{\ell,\mathrm{f}}\rangle_{n/d}^{\mathrm{new}}\langle\pi_d(\mathcal{D}_{n,d})\rangle_d^{\mathrm{new}} = \sum_{d|n_+}\langle(\kappa_{n/d})_{\ell,\mathrm{f}}\rangle_{n/d}^{\mathrm{new}}\mathcal{D}_d = 0.$$

Finally, suppose that $\ell|n/n_+$. Using Definition 6.2(v) and property (a) above,

$$\tilde\kappa_n = \langle\tilde\kappa_n\rangle_n^{\mathrm{new}} = \sum_{d|n_+}\langle(\kappa_{n/d})\rangle_{n/d}^{\mathrm{new}}\mathcal{D}_d = \sum_{d|(n/\ell)_+}\langle(\kappa_{n/(d\ell)})\rangle_{n/(d\ell)}^{\mathrm{new}}\mathcal{D}_d = \langle\tilde\kappa_{n/\ell}\rangle_{n/\ell}^{\mathrm{new}} = \tilde\kappa_{n/\ell}.$$

This completes the proof that $\tilde{\boldsymbol{\kappa}}$ is a Kolyvagin system.

Since $\mathbf{KS}(F)$ is a free $\mathbb{Z}_p$-module of rank one [MR04a, Theorem 5.2.10(ii)], to complete the proof it remains only to show that the map $\mathbf{PKS}(F)\to\mathbf{KS}(F)$ is surjective. If $\tilde{\boldsymbol{\kappa}}\in\mathbf{KS}(F)$, then (since $\mathcal{D}_{n,1}=1$) we can define inductively a collection $\boldsymbol{\kappa}:=\{\kappa_n\in(\hat F^\times)^-\otimes I_n^r/I_n^{r+1} : n\in\mathcal{N}_p\}$ such that $\sum_{d|n_+}\kappa_{n/d}\,\mathcal{D}_{n,d}=\tilde\kappa_n$ for every n. It is straightforward to check that $\boldsymbol{\kappa}$ is a pre-Kolyvagin system; since we will not make use of this, we omit the proof. By Definition 6.3 the image of $\boldsymbol{\kappa}$ in $\mathbf{KS}(F)$ is $\tilde{\boldsymbol{\kappa}}$. □

Corollary 6.6. *Suppose $\boldsymbol{\kappa},\boldsymbol{\kappa}'\in\mathbf{PKS}(F)$. If $\kappa_1=\kappa_1'$, then $\kappa_n=\kappa_n'$ for every $n\in\mathcal{N}_p$.*

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

Proof. Let $\tilde{\boldsymbol{\kappa}}$ and $\tilde{\boldsymbol{\kappa}}'$ be the images of $\boldsymbol{\kappa}$ and $\boldsymbol{\kappa}'$, respectively, under the map of Definition 6.3. Then $\tilde{\boldsymbol{\kappa}}$ and $\tilde{\boldsymbol{\kappa}}'$ are Kolyvagin systems, and $\tilde{\kappa}_1 = \kappa_1 = \kappa_1' = \tilde{\kappa}_1'$. Therefore $\tilde{\boldsymbol{\kappa}} = \tilde{\boldsymbol{\kappa}}'$ by Theorem 5.4, so by the injectivity assertion of Proposition 6.5 we have $\boldsymbol{\kappa} = \boldsymbol{\kappa}'$, i.e. $\kappa_n = \kappa_n'$ for every $n \in \mathcal{N}_p$. □

We will use the following definition and lemma to replace property (iv) in the definition of a pre-Kolyvagin system by an equivalent property that will be easier to verify. See Remark 6.9 below.

Definition 6.7. If $n \in \mathcal{N}$, let $\mathfrak{S}(n)$ denote the set of permutations of the primes dividing n_+, and let $\mathfrak{S}_1(n) \subset \mathfrak{S}(n)$ be the subset

$$\mathfrak{S}_1(n) := \{\sigma \in \mathfrak{S}(n) : \text{the primes not fixed by } \sigma \text{ form a single } \sigma\text{-orbit}\}.$$

If $\sigma \in \mathfrak{S}(n)$ let $d_\sigma := \prod_{\ell \mid n_+, \sigma(\ell) \neq \ell} \ell$, the product of the primes not fixed by σ, and define

$$\Pi(\sigma) := \prod_{q \mid d_\sigma} \pi_q(\mathrm{Fr}_{\sigma(q)} - 1).$$

Lemma 6.8. *Suppose that A is an abelian group, ℓ is a prime that splits in $F/\mathbb{Q}$, and $x_n \in A \otimes \mathcal{I}_n^{\mathrm{new}}$ for every $n \in \mathcal{N}_p$. Then the following are equivalent:*

(i) *for every n divisible by ℓ, $\sum_{d \mid n_+} x_{n/d}\, \mathcal{D}_d = 0$;*

(ii) *for every n divisible by ℓ, $x_n = -\sum_{\substack{\sigma \in \mathfrak{S}_1(n) \\ \sigma(\ell) \neq \ell}} \mathrm{sign}(\sigma) x_{n/d_\sigma} \Pi(\sigma)$.*

Proof. We show first that property (ii) implies property (i) (which is the implication we use later in this paper). Let $\mathfrak{S}'(d) \subset \mathfrak{S}(d)$ denote the derangements, i.e. the permutations with no fixed points. Then we can evaluate the determinant $\mathcal{D}_d = \det(M_d)$ as follows. Let $m_{q,q'}$ be the (q, q')-entry in M_d. Then

$$\mathcal{D}_d = \sum_{\sigma \in \mathfrak{S}(d)} \mathrm{sign}(\sigma) \prod_{q \mid d} m_{q,\sigma(q)} = \sum_{\sigma \in \mathfrak{S}'(d)} \mathrm{sign}(\sigma) \Pi(\sigma), \tag{5}$$

where the second equality holds since the diagonal entries of M_d vanish.

Fix an n divisible by ℓ, and let

$$S_1 = \sum_{d \mid n_+, \ell \nmid d} x_{n/d}\, \mathcal{D}_d, \quad S_2 = \sum_{d \mid n_+, \ell \mid d} x_{n/d}\, \mathcal{D}_d.$$

Using property (ii) we have

$$S_1 = -\sum_{\substack{d \mid n_+ \\ \ell \nmid d}} \sum_{\substack{\sigma \in \mathfrak{S}_1(n/d) \\ \sigma(\ell) \neq \ell}} \mathrm{sign}(\sigma) \langle (x_{n/(dd_\sigma)})_\ell \rangle^{\mathrm{new}}_{n/(dd_\sigma)} \Pi(\sigma) \mathcal{D}_d. \tag{6}$$

Fix a divisor δ of n_+ that is divisible by ℓ. We will show that the coefficient of $x_{n/\delta}$ in S_1 in (6) is $-\mathcal{D}_\delta$, which exactly cancels the coefficient of $x_{n/\delta}$ in S_2. Using (5), the coefficient of $x_{n/\delta}$ in S_1 in (6) is

$$\begin{aligned} &-\sum_{d \mid (\delta/\ell)} \sum_{\substack{\sigma \in \mathfrak{S}_1(n/d) \\ d_\sigma = \delta/d}} \left(\mathrm{sign}(\sigma) \Pi(\sigma) \sum_{\eta \in \mathfrak{S}'(d)} \mathrm{sign}(\eta) \Pi(\eta) \right) \\ &\quad = -\sum_{d \mid (\delta/\ell)} \sum_{\substack{\sigma \in \mathfrak{S}_1(n/d) \\ d_\sigma = \delta/d}} \sum_{\eta \in \mathfrak{S}'(d)} \mathrm{sign}(\sigma\eta) \Pi(\sigma\eta). \end{aligned}$$

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

For every $\rho \in \mathfrak{S}'(\delta)$ there is a unique triple (d, σ, η) such that

$$d|\delta/\ell, \sigma \in \mathfrak{S}_1(n/d), d_\sigma = \delta/d, \eta \in \mathfrak{S}'(d) \quad \text{and} \quad \rho = \sigma\eta.$$

To see this, simply write ρ as a product of disjoint cycles, let σ be the cycle containing ℓ, and let $d = \delta/d_\sigma$ and $\eta = \sigma^{-1}\rho$. Thus the coefficient of $x_{n/\delta}$ in S_1 in (6) is (using (5) again)

$$-\sum_{\rho \in \mathfrak{S}'(\delta)} \operatorname{sign}(\rho)\Pi(\rho) = -\mathcal{D}_\delta.$$

Therefore $\sum_{d|n_+} x_{n/d}\,\mathcal{D}_d = S_1 + S_2 = 0$, so property (i) holds.

Although we will not need it, here is a simple argument to show that property (i) implies property (ii). Suppose that $X := \{x_n \in A \otimes \mathcal{I}_n^{\text{new}} : n \in \mathcal{N}_p\}$ satisfies property (i). If $\ell|n$, then (since $\mathcal{D}_1 = 1$) we can use property (i) recursively to express x_n as a linear combination of x_d with $\ell \nmid d$. Thus X is uniquely determined by the subset $X' := \{x_n \in A \otimes \mathcal{I}_n^{\text{new}} : n \in \mathcal{N}_p, \ell \nmid n\}$. Clearly X' determines a unique collection $Y := \{y_n \in A \otimes \mathcal{I}_n^{\text{new}} : n \in \mathcal{N}_p\}$ satisfying property (ii), with $y_n = x_n$ if $\ell \nmid n$. We showed above that property (ii) implies property (i), so Y satisfies property (i). Since (i) and X' uniquely determine both X and Y, we must have $X = Y$, and so X satisfies property (ii). □

Remark 6.9. We will apply Lemma 6.8 as follows. Let $A := (\hat{F}_{\ell,\mathrm{f}}^\times)^-$, and let $x_n := \langle(\kappa_n)_{\ell,\mathrm{f}}\rangle_n^{\text{new}}$. Then Lemma 6.8 says that we can replace property (iv) of Definition 6.2 of a pre-Kolyvagin system by the equivalent statement:

(iv)′ if $\ell|n_+$, then

$$\langle(\kappa_n)_{\ell,\mathrm{f}}\rangle_n^{\text{new}} = -\sum_{\substack{\sigma \in \mathfrak{S}_1(n) \\ \sigma(\ell) \neq \ell}} \operatorname{sign}(\sigma)\langle(\kappa_{n/d_\sigma})_\ell\rangle_{n/d_\sigma}^{\text{new}}\Pi(\sigma).$$

7. The cyclotomic unit pre-Kolyvagin system

Fix an odd prime p. If $n \in \mathcal{N}$, let $s(n)$ be the number of prime factors of n/n_+. In this section we will show that the collection $\{2^{-s(n)}\tilde{\theta}'_n : n \in \mathcal{N}_p\}$ is a pre-Kolyvagin system. Recall that

$$\mathcal{N}_p^+ := \{n \in \mathcal{N}_p : \text{all } \ell|n \text{ split in } F/\mathbb{Q}\}.$$

Proposition 7.1 (Darmon). *If $n \in \mathcal{N}_p$ then*

$$\sum_{d|n_+} \tilde{\theta}'_{n/d} \prod_{\ell|d} \pi_{n/d}(\mathrm{Fr}_\ell - 1) = 2^{s(n)}\beta_{n_+} \quad \text{in } (\hat{F}^\times)^- \otimes \mathcal{I}_n^{\text{new}}$$

where, for $n \in \mathcal{N}_p^+$, $\beta_n \in (\hat{F}^\times)^- \otimes \mathcal{I}_n^{\text{new}}$ is the Kolyvagin derivative class denoted $\kappa(n)$ in [Dar95, § 6], or κ_n in [MR04b, Appendix].

Proof. This is [Dar95, Proposition 9.4].[1] (Note that $\kappa(n)$ in [Dar95, § 6] and κ_n in [MR04b, Appendix] are defined to lie in $(\hat{F}^\times)^- \otimes (\mathbb{Z}/\gcd(\ell - 1 : \ell|n)\mathbb{Z})$, after fixing generators of every Γ_ℓ. Without fixing such choices, the elements defined in [Dar95, MR04b] live naturally in $(\hat{F}^\times)^- \otimes \mathcal{I}_n^{\text{new}}$.) □

Theorem 7.2. *The collection $\{2^{-s(n)}\tilde{\theta}'_n : n \in \mathcal{N}_p\}$ is a pre-Kolyvagin system.*

[1] There is a typo in [Dar95, Proposition 9.4]. The last two T's should be TQ, as in [Dar95, Lemma 8.1].

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

Proof. We need to check the five properties of Definition 6.2. For $n \in \mathcal{N}_p^+$, let β_n be as in Proposition 7.1.

Since $\beta_{n_+} \in (\hat{F}^\times)^- \otimes \mathcal{I}_n^{\text{new}}$ for every n, it follows easily by induction from Proposition 7.1 that $\tilde{\theta}'_n \in (\hat{F}^\times)^- \otimes I_n^r/I_n^{r+1}$, where r is the number of prime factors of n_+. This is (i) of Definition 6.2.

Suppose $\ell | n_+$. A standard property of cyclotomic units shows that

$$\mathbb{N}_{F(\boldsymbol{\mu}_n)/F(\boldsymbol{\mu}_{n/\ell})}\alpha_n = \alpha_{n/\ell}/\alpha_{n/\ell}^{\mathrm{Fr}_\ell^{-1}}.$$

It follows from the definition of θ'_n that

$$\begin{aligned}(1 \otimes \pi_{n/\ell})(\theta'_n) &= \sum_{\gamma \in \Gamma_n} \gamma(\alpha_n) \otimes \pi_{n/\ell}(\gamma) = \sum_{\gamma \in \Gamma_{n/\ell}} \gamma(\mathbb{N}_{F(\boldsymbol{\mu}_n)/F(\boldsymbol{\mu}_{n/\ell})}\alpha_n) \otimes \gamma \\ &= \sum_{\gamma \in \Gamma_{n/\ell}} \gamma(\alpha_{n/\ell}/\alpha_{n/\ell}^{\mathrm{Fr}_\ell^{-1}}) \otimes \gamma = \sum_{\gamma \in \Gamma_{n/\ell}} \gamma(\alpha_{n/\ell}) \otimes \gamma\, \pi_{n/\ell}(1 - \mathrm{Fr}_\ell) \\ &= \theta'_{n/\ell}\, \pi_{n/\ell}(1 - \mathrm{Fr}_\ell).\end{aligned}$$

Since $\ell | n_+$ we have $s(n) = s(n/\ell)$, so this verifies property (ii) of Definition 6.2.

Projecting each of the summands in Proposition 7.1 into $(\hat{F}^\times)^- \otimes \mathcal{I}_n^{\text{new}}$, one sees that all terms with $d > 1$ vanish, yielding

$$\langle 2^{-s(n)}\tilde{\theta}'_n \rangle_n^{\text{new}} = \langle \beta_{n_+} \rangle_n^{\text{new}} = \beta_{n_+}.$$

Properties (iii), (iv), and (v) of Definition 6.2 follow from the corresponding properties of the β_{n_+}. See [MR04a, Proposition A.2] or [Rub00, Theorem 4.5.4] for property (iii), and [MR04a, Theorem A.4] or [MR04b, Proposition A.2] for property (iv)′ of Remark 6.9. Property (v) is immediate, since β_{n_+} depends only on n_+. □

8. The regulator pre-Kolyvagin system

In this section we study relations among the regulator elements R_n, to show that the collection $\{h_n R_n : n \in \mathcal{N}_p\}$ is a pre-Kolyvagin system.

Lemma 8.1. *Suppose $n \in \mathcal{N}$, $\ell | n_+$, and $\{\lambda_0 - \lambda_0^\tau, \dots, \lambda_r - \lambda_r^\tau\}$ is a standard basis of X_n^- with $\lambda_r \lambda_r^\tau = \ell$. Then $\{\lambda_0 - \lambda_0^\tau, \dots, \lambda_{r-1} - \lambda_{r-1}^\tau\}$ is a standard basis of $X_{n/\ell}^-$, and we can choose an oriented basis $\{\epsilon_0, \dots, \epsilon_r\}$ of $(1-\tau)\mathcal{E}_n$ such that $\{\epsilon_0, \dots, \epsilon_{r-1}\}$ is an oriented basis of $(1-\tau)\mathcal{E}_{n/\ell}$.*

With any such bases, $\mathrm{ord}_{\lambda_r}(\epsilon_r) = -h_{n/\ell}/h_n$ and

$$[\epsilon_r]_{\lambda_r}^{n/\ell} = \frac{h_{n/\ell}}{h_n}\, \pi_{n/\ell}(1 - \mathrm{Fr}_\ell) \in I_{n/\ell}/I_{n/\ell}^2.$$

Proof. Everything except the final sentence is clear. Comparing the determinants of the logarithmic embeddings

$$(1-\tau)\mathcal{E}_{n/\ell} \xrightarrow{\xi_{n/\ell}} X_{n/\ell}^-, \quad (1-\tau)\mathcal{E}_n \xrightarrow{\xi_n} X_n^-$$

with respect to our given bases, we see that

$$\det(\xi_n) = \log |\epsilon_r|_{\lambda_r} \det(\xi_{n/\ell})$$

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

because $\log|\epsilon_i|_{\lambda_r}=0$ for $0\leqslant i<r$. Since our bases are oriented, both determinants are positive. Hence

$$|\epsilon_r|_{\lambda_r}=\ell^{-\mathrm{ord}_{\lambda_r}(\epsilon_r)}>1$$

so $\mathrm{ord}_{\lambda_r}(\epsilon_r)<0$.

The exact sequence

$$(1-\tau)\mathcal{E}_n\xrightarrow{\mathrm{ord}_{\lambda_r}}\mathbb{Z}\xrightarrow{\cdot\lambda_r}\mathrm{Pic}(\mathcal{O}_F[\ell/n])\longrightarrow\mathrm{Pic}(\mathcal{O}_F[1/n])\longrightarrow 0$$

shows that

$$[\mathbb{Z}:\mathrm{ord}_{\lambda_r}(\epsilon_r)\mathbb{Z}]=h_{n/\ell}/h_n,$$

so $\mathrm{ord}_{\lambda_r}(\epsilon_r)=-h_{n/\ell}/h_n$ as claimed. Since $F(\boldsymbol{\mu}_{n/\ell})/F$ is unramified at λ_r,

$$[\epsilon_r]_{\lambda_r}^{n/\ell}=(\mathrm{Fr}_\ell^{\mathrm{ord}_{\lambda_r}(\epsilon_r)})-1=\mathrm{ord}_{\lambda_r}(\epsilon_r)(\mathrm{Fr}_\ell-1)=-h_{n/\ell}/h_n(\mathrm{Fr}_\ell-1)$$

in $I_{n/\ell}/I_{n/\ell}^2$. □

Proposition 8.2. *Suppose $n\in\mathcal{N}$, $\ell|n_+$, and $r=r(n)$. Then*

$$(1\otimes\pi_{n/\ell})(h_nR_n)=h_{n/\ell}R_{n/\ell}\,\pi_{n/\ell}(1-\mathrm{Fr}_\ell)\in F^\times\otimes I_n^r/I_n^{r+1}.$$

Proof. To compute R_n, fix bases for X_n^- and $\mathcal{E}_n^-$ as in Lemma 8.1. By definition

$$R_n:=\begin{vmatrix}\epsilon_0 & \epsilon_1 & \cdots & \epsilon_r\\ [\epsilon_0]_{\lambda_1}^n & [\epsilon_1]_{\lambda_1}^n & \cdots & [\epsilon_r]_{\lambda_1}^n\\ \vdots & \vdots & & \vdots\\ [\epsilon_0]_{\lambda_r}^n & [\epsilon_1]_{\lambda_r}^n & \cdots & [\epsilon_r]_{\lambda_r}^n\end{vmatrix},$$

and then $(1\otimes\pi_{n/\ell})(R_n)$ is the determinant of the matrix obtained by applying $\pi_{n/\ell}$ to rows 2 through $r+1$ of this matrix. For $i<r$, ϵ_i is a unit at λ_r, so the local Artin symbol $[\epsilon_i,F(\boldsymbol{\mu}_n)_{\lambda_r}/F_{\lambda_r}]$ lies in the inertia group Γ_ℓ. Hence $\pi_{n/\ell}([\epsilon_i]_{\lambda_r}^n)=[\epsilon_i]_{\lambda_r}^{n/\ell}=0$ for $i<r$, and so

$$(1\otimes\pi_{n/\ell})(R_n)=\begin{vmatrix}\epsilon_0 & \cdots & \epsilon_{r-1} & \epsilon_r\\ [\epsilon_0]_{\lambda_1}^{n/\ell} & \cdots & [\epsilon_{r-1}]_{\lambda_1}^{n/\ell} & [\epsilon_r]_{\lambda_1}^{n/\ell}\\ \vdots & & \vdots & \vdots\\ [\epsilon_0]_{\lambda_{r-1}}^{n/\ell} & \cdots & [\epsilon_{r-1}]_{\lambda_{r-1}}^{n/\ell} & [\epsilon_r]_{\lambda_{r-1}}^{n/\ell}\\ 0 & \cdots & 0 & [\epsilon_r]_{\lambda_r}^{n/\ell}\end{vmatrix}.$$

The upper left $r\times r$ determinant is the one used to define $R_{n/\ell}$, so

$$(1\otimes\pi_{n/\ell})(R_n)=R_{n/\ell}[\epsilon_r]_{\lambda_r}^{n/\ell}=\frac{h_{n/\ell}}{h_n}R_{n/\ell}\,\pi_{n/\ell}(1-\mathrm{Fr}_\ell)$$

by Lemma 8.1. □

Fix an odd prime p as in §§ 5 and 6, and keep the rest of the notation of those sections as well.

Lemma 8.3. *If $n\in\mathcal{N}_p$, ℓ is a prime not dividing n, and $r=r(n)$, then*

$$(R_n)_\ell\in(\hat{F}_{\ell,\mathrm{f}}^\times)^-\otimes I_n^r/I_n^{r+1}.$$

Proof. Since $\ell\nmid n$, if $\epsilon\in\mathcal{E}_n^-$ then $\epsilon_\ell\in(\hat{\mathcal{O}}_\ell^\times)^-=(\hat{F}_{\ell,\mathrm{f}}^\times)^-\subset(\hat{F}_\ell^\times)^-$. Now the lemma is clear, since $R_n\in\mathcal{E}_n^-\otimes I_n^r/I_n^{r+1}$. □

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

Proposition 8.4. *Suppose $n \in \mathcal{N}_p$ and $\ell | n_+$. Then*

$$\langle h_n(R_n)_{\ell,\mathrm{tr}} \rangle_n^{\mathrm{new}} = (\phi_\ell^{\mathrm{fs}} \otimes 1)(\langle h_{n/\ell}(R_{n/\ell})_\ell \rangle_{n/\ell}^{\mathrm{new}}).$$

Proof. Note that $(\phi_\ell^{\mathrm{fs}} \otimes 1)(\langle h_{n/\ell}(R_{n/\ell})_\ell \rangle_{n/\ell}^{\mathrm{new}}) \in (\hat{F}_{\ell,\mathrm{tr}}^\times)^- \otimes \mathcal{I}_n^{\mathrm{new}}$ is well-defined, since Lemma 8.3 shows that $(R_{n/\ell})_\ell \in (\hat{F}_{\ell,\mathrm{f}}^\times)^- \otimes I_{n/\ell}^{r-1}/I_{n/\ell}^r$.

As in the proof of Proposition 8.2, fix a basis $\{\lambda_0 - \lambda_0^\tau, \dots, \lambda_r - \lambda_r^\tau\}$ of X_n^- with $\ell = \lambda_r \lambda_r^\tau$, and an oriented basis $\{\epsilon_0, \dots, \epsilon_r\}$ of $(1-\tau)\mathcal{E}_n$ as in Lemma 8.1. Then

$$(R_n)_{\ell,\mathrm{tr}} = \begin{vmatrix} (\epsilon_0)_{\ell,\mathrm{tr}} & \cdots & (\epsilon_{r-1})_{\ell,\mathrm{tr}} & (\epsilon_r)_{\ell,\mathrm{tr}} \\ [\epsilon_0]_{\lambda_1}^n & [\epsilon_1]_{\lambda_1}^n & \cdots & [\epsilon_r]_{\lambda_1}^n \\ \vdots & \vdots & & \vdots \\ [\epsilon_0]_{\lambda_r}^n & [\epsilon_1]_{\lambda_r}^n & \cdots & [\epsilon_r]_{\lambda_r}^n \end{vmatrix} = \mathrm{ord}_{\lambda_r}(\epsilon_r) \begin{vmatrix} 1 & \cdots & 1 & (\ell, \ell^{-1}) \\ [\epsilon_0]_{\lambda_1}^n & [\epsilon_1]_{\lambda_1}^n & \cdots & [\epsilon_r]_{\lambda_1}^n \\ \vdots & \vdots & & \vdots \\ [\epsilon_0]_{\lambda_r}^n & [\epsilon_1]_{\lambda_r}^n & \cdots & [\epsilon_r]_{\lambda_r}^n \end{vmatrix}$$

since $(\epsilon_r)_{\ell,\mathrm{tr}} = (\ell, \ell^{-1})^{\mathrm{ord}_{\lambda_r}(\epsilon_r)}$, and $(\epsilon_i)_{\ell,\mathrm{tr}} = 1$ for $i < r$. (Recall that when we evaluate these determinants using (2), the multiplicative notation in $(\hat{F}_\ell^\times)_{\mathrm{tr}}$ changes to additive notation in the tensor product $(\hat{F}_\ell^\times)_{\mathrm{tr}} \otimes I_\ell^r/I_\ell^{r+1}$, so the 1's in the top row become 0's, and $(\ell, \ell^{-1})^{\mathrm{ord}_{\lambda_r}(\epsilon_r)}$ becomes $\mathrm{ord}_{\lambda_r}(\epsilon_r) \cdot (\ell, \ell^{-1})$.) We have $\mathrm{ord}_{\lambda_r}(\epsilon_r) = -h_{n/\ell}/h_n$ by Lemma 8.1. For $i < r$ we have $\mathrm{ord}_{\lambda_r}(\epsilon_i) = 0$, so $[\epsilon_i]_{\lambda_r}^n = [\epsilon_i]_{\lambda_r}^\ell \in I_\ell/I_\ell^2$ and

$$\phi_\ell^{\mathrm{fs}}((\epsilon_i)_\ell) = (\ell, \ell^{-1}) \otimes [\epsilon_i]_{\lambda_r}^n \in (\hat{F}_\ell^\times)_{\mathrm{tr}} \otimes I_\ell/I_\ell^2.$$

Thus

$$(R_n)_{\ell,\mathrm{tr}} = -\frac{h_{n/\ell}}{h_n}(-1)^r(-1)^{r-1} \begin{vmatrix} \phi_\ell^{\mathrm{fs}}((\epsilon_0)_\ell) & \cdots & \phi_\ell^{\mathrm{fs}}((\epsilon_{r-1})_\ell) \\ [\epsilon_0]_{\lambda_1}^n & \cdots & [\epsilon_{r-1}]_{\lambda_1}^n \\ \vdots & \vdots & \vdots \\ [\epsilon_0]_{\lambda_{r-1}}^n & \cdots & [\epsilon_{r-1}]_{\lambda_{r-1}}^n \end{vmatrix}$$

$$= \frac{h_{n/\ell}}{h_n} \begin{vmatrix} \phi_\ell^{\mathrm{fs}}((\epsilon_0)_\ell) & \cdots & \phi_\ell^{\mathrm{fs}}((\epsilon_{r-1})_\ell) \\ [\epsilon_0]_{\lambda_1}^{n/\ell} + [\epsilon_0]_{\lambda_1}^\ell & \cdots & [\epsilon_{r-1}]_{\lambda_1}^{n/\ell} + [\epsilon_{r-1}]_{\lambda_1}^\ell \\ \vdots & \vdots & \vdots \\ [\epsilon_0]_{\lambda_{r-1}}^{n/\ell} + [\epsilon_0]_{\lambda_{r-1}}^\ell & \cdots & [\epsilon_{r-1}]_{\lambda_{r-1}}^{n/\ell} + [\epsilon_{r-1}]_{\lambda_{r-1}}^\ell \end{vmatrix}$$

(we have the $(-1)^r$ because we moved column $r+1$ to column 1, and the $(-1)^{r-1}$ because we moved row $r+1$ to row 2). When we expand the last determinant (including expanding the sums $[\epsilon_i]_{\lambda_j}^{n/\ell} + [\epsilon_i]_{\lambda_j}^\ell$), each term that includes one of the $[\epsilon_i]_{\lambda_j}^\ell$ lies in I_ℓ^2 (since the top row also contributes one element of I_ℓ). Thus all such terms project to zero in $\mathcal{I}_n^{\mathrm{new}}$, and so

$$\langle (R_n)_{\ell,\mathrm{tr}} \rangle_n^{\mathrm{new}} = \frac{h_{n/\ell}}{h_n} \langle \det(A) \rangle_n^{\mathrm{new}}$$

where

$$A = \begin{bmatrix} \phi_\ell^{\mathrm{fs}}((\epsilon_0)_\ell) & \cdots & \phi_\ell^{\mathrm{fs}}((\epsilon_{r-1})_\ell) \\ [\epsilon_0]_{\lambda_1}^{n/\ell} & \cdots & [\epsilon_{r-1}]_{\lambda_1}^{n/\ell} \\ \vdots & \vdots & \vdots \\ [\epsilon_0]_{\lambda_{r-1}}^{n/\ell} & \cdots & [\epsilon_{r-1}]_{\lambda_{r-1}}^{n/\ell} \end{bmatrix}.$$

But then $\det(A) = (\phi_\ell^{\mathrm{fs}} \otimes 1)((R_{n/\ell})_\ell)$, so the proposition follows. □

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

Suppose $n, n' \in \mathcal{N}$, $n|n'$, and $r = r(n)$. Define

$$S_{n,n'} := \begin{vmatrix} \epsilon_0 & \epsilon_1 & \cdots & \epsilon_r \\ [\epsilon_0]_{\lambda_1}^{n'} & [\epsilon_1]_{\lambda_1}^{n'} & \cdots & [\epsilon_r]_{\lambda_1}^{n'} \\ \vdots & \vdots & & \vdots \\ [\epsilon_0]_{\lambda_r}^{n'} & [\epsilon_1]_{\lambda_r}^{n'} & \cdots & [\epsilon_r]_{\lambda_r}^{n'} \end{vmatrix} \in \mathcal{E}_n^- \otimes I_{n'}^r / I_{n'}^{r+1},$$

using any standard basis of X_n^- and oriented basis of $(1-\tau)\mathcal{E}_n$. In particular $S_{n,n} = R_n$.

Proposition 8.5. *Suppose $n \in \mathcal{N}$ and $\ell \nmid n$.*

(i) *If ℓ is inert in $F/\mathbb{Q}$, then $h_{n\ell}\langle R_{n\ell}\rangle_n^{\mathrm{new}} = h_n \langle R_n \rangle_n^{\mathrm{new}}$.*

(ii) *If ℓ splits in $F/\mathbb{Q}$ and $v \in I_n$, then*

$$h_n \langle S_{n,n\ell}\, v\rangle_{n\ell}^{\mathrm{new}} = \langle R_n \rangle_n^{\mathrm{new}} \pi_\ell(v) - \sum_{\text{primes } q|n_+} h_{n/q} \langle S_{n/q,n}\, v\rangle_n^{\mathrm{new}} \pi_\ell(\mathrm{Fr}_q - 1)$$

in $\mathcal{E}_n^- \otimes \mathcal{I}_{n\ell}^{\mathrm{new}}$.

Proof. Let r be the number of prime divisors of n_+, so X_n^- and $(1-\tau)\mathcal{E}_n$ are free $\mathbb{Z}$-modules of rank $r+1$. Choose a standard basis of X_n^- and an oriented basis of $(1-\tau)\mathcal{E}_n$. For $1 \leqslant i \leqslant r = r(n)$, let

$$a_i = ([\epsilon_0]_{\lambda_i}^n, [\epsilon_1]_{\lambda_i}^n, \ldots, [\epsilon_r]_{\lambda_i}^n), \quad b_i = ([\epsilon_0]_{\lambda_i}^\ell, [\epsilon_1]_{\lambda_i}^\ell, \ldots, [\epsilon_r]_{\lambda_i}^\ell).$$

Then

$$S_{n,n\ell} = \begin{vmatrix} \epsilon_0 & \cdots & \epsilon_r \\ & a_1 + b_1 & \\ & \vdots & \\ & a_r + b_r & \end{vmatrix} = \sum_{T \subset \{1,\ldots,r\}} \det(A_T) \tag{7}$$

where A_T is the matrix whose top row is $(\epsilon_0, \ldots, \epsilon_r)$ and whose $(i+1)$th row for $1 \leqslant i \leqslant r$ is b_i if $i \in T$ and a_i if $i \notin T$. Note that $\det(A_\emptyset) = R_n$, and that the entries of each b_i are in I_ℓ / I_ℓ^2.

Suppose first that ℓ is inert in $F/\mathbb{Q}$, so $(n\ell)_+ = n_+$. Then $\langle \det(A_T)\rangle_n^{\mathrm{new}} = 0$ if T is non-empty (since $\mathcal{I}_n^{\mathrm{new}}$ has no 'ℓ component'), so (7) shows that

$$\langle S_{n,n\ell}\rangle_n^{\mathrm{new}} = \langle \det(A_\emptyset)\rangle_n^{\mathrm{new}} = \langle R_n \rangle_n^{\mathrm{new}}.$$

Further, since ℓ is inert in $F/\mathbb{Q}$ we have $X_{n\ell}^- = X_n^-$, $(1-\tau)\mathcal{E}_{n\ell} = (1-\tau)\mathcal{E}_n$, and $h_{n\ell} = h_n$. Thus $S_{n,n\ell} = R_{n\ell}$, and so

$$h_{n\ell}\langle R_{n\ell}\rangle_{(n\ell)}^{\mathrm{new}} = h_n \langle S_{n,n\ell}\rangle_n^{\mathrm{new}} = h_n \langle R_n \rangle_n^{\mathrm{new}}.$$

This is assertion (i).

Now suppose that ℓ splits in $F/\mathbb{Q}$. Since the entries of each b_i are in I_ℓ, if $\#(T) \geqslant 2$ we have $\langle \det(A_T) v\rangle_{n\ell}^{\mathrm{new}} = 0$. Thus (7) gives

$$\langle S_{n,n\ell}\, v\rangle_{n\ell}^{\mathrm{new}} = \langle \det(A_\emptyset) v\rangle_{n\ell}^{\mathrm{new}} + \sum_{i=1}^r \langle \det(A_{\{i\}}) v\rangle_{n\ell}^{\mathrm{new}}. \tag{8}$$

By definition of R_n,

$$\langle \det(A_\emptyset) v\rangle_{n\ell}^{\mathrm{new}} = \langle R_n v\rangle_{n\ell}^{\mathrm{new}} = \langle R_n \rangle_n^{\mathrm{new}} \pi_\ell(v). \tag{9}$$

To compute $\det(A_{\{i\}})$, let $q = \lambda_i \lambda_i^\tau$, and assume that our oriented basis of $(1-\tau)\mathcal{E}_n$ was chosen so that $\{\epsilon_0, \ldots, \epsilon_{r-1}\}$ is an oriented basis of $(1-\tau)\mathcal{E}_{n/q}$ with respect to the standard

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

basis of $X_{n/q}$ obtained by removing $\lambda_i - \lambda_i^\tau$ from $\{\lambda_1 - \lambda_1^\tau, \dots, \lambda_r - \lambda_r^\tau\}$. For $1 \leqslant j \leqslant r-1$, ϵ_j is a unit at λ_i, so $[\epsilon_j]^\ell_{\lambda_i} = 0$. Thus

$$\det(A_{\{i\}}) = \begin{vmatrix} \epsilon_0 & \cdots & \epsilon_{r-1} & \epsilon_r \\ [\epsilon_0]^n_{\lambda_1} & \cdots & [\epsilon_{r-1}]^n_{\lambda_1} & [\epsilon_r]^n_{\lambda_1} \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & [\epsilon_r]^\ell_{\lambda_i} \\ \vdots & & \vdots & \vdots \\ [\epsilon_0]^n_{\lambda_r} & \cdots & [\epsilon_{r-1}]^n_{\lambda_r} & [\epsilon_r]^n_{\lambda_r} \end{vmatrix} = (-1)^{r+i} \begin{vmatrix} \epsilon_0 & \cdots & \epsilon_{r-1} \\ [\epsilon_0]^n_{\lambda_1} & \cdots & [\epsilon_{r-1}]^n_{\lambda_1} \\ \vdots & \vdots & \vdots \\ [\epsilon_0]^n_{\lambda_r} & \cdots & [\epsilon_{r-1}]^n_{\lambda_r} \end{vmatrix} [\epsilon_r]^\ell_{\lambda_i}$$
$$= (-1)^{r+i} S_{n/q,n}\, [\epsilon_r]^\ell_{\lambda_i}$$

(where the second determinant has no λ_i row). Further, an argument identical to that of Lemma 8.1 shows that

$$[\epsilon_r]^\ell_{\lambda_i} = (-1)^{r+i+1} \frac{h_{n/q}}{h_n}\, \pi_\ell(\mathrm{Fr}_q - 1) \in I_\ell / I_\ell^2.$$

Therefore

$$\det(A_{\{i\}}) = -\frac{h_{n/q}}{h_n} S_{n/q,n}\, \pi_\ell(\mathrm{Fr}_q - 1).$$

Multiplying (8) by h_n and using (9) gives

$$h_n \langle S_{n,n\ell} v \rangle^{\mathrm{new}}_{n\ell} = h_n \langle R_n \rangle^{\mathrm{new}}_n\, \pi_\ell(v) - \sum_{q \mid n_+} h_{n/q} \langle S_{n/q,n} v \pi_\ell(\mathrm{Fr}_q - 1) \rangle^{\mathrm{new}}_{n\ell}.$$

Since $S_{n/q,n} \in I_n^r / I_n^{r+1}$, we have

$$\langle S_{n/q,n} v \pi_\ell(\mathrm{Fr}_q - 1) \rangle^{\mathrm{new}}_{n\ell} = \langle S_{n/q,n}\, \pi_n(v) \rangle^{\mathrm{new}}_n\, \pi_\ell(\mathrm{Fr}_q - 1).$$

This completes the proof of the proposition. □

If $n \in \mathcal{N}$, recall (Definition 6.7) that $\mathfrak{S}(n)$ denotes the set of permutations of the primes dividing n_+, $\mathfrak{S}_1(n) \subset \mathfrak{S}(n)$ is the subset

$$\mathfrak{S}_1(n) := \{\sigma \in \mathfrak{S}(n) : \text{the primes not fixed by } \sigma \text{ form a single } \sigma\text{-orbit}\},$$

and if $\sigma \in \mathfrak{S}(n)$ then $d_\sigma := \prod_{\sigma(\ell) \neq \ell} \ell$ and $\Pi(\sigma) := \prod_{q \mid d_\sigma} \pi_q(\mathrm{Fr}_{\sigma(q)} - 1)$.

Theorem 8.6. *If $n \in \mathcal{N}_p$ and $\ell \mid n_+$, then*

$$\langle h_n (R_n)_{\ell,\mathrm{f}} \rangle^{\mathrm{new}}_n = - \sum_{\substack{\sigma \in \mathfrak{S}_1(n) \\ \sigma(\ell) \neq \ell}} \mathrm{sign}(\sigma) \langle h_{n/d_\sigma} (R_{n/d_\sigma})_\ell \rangle^{\mathrm{new}}_{n/d_\sigma} \Pi(\sigma).$$

Proof. As usual, fix a basis $\{\lambda_0 - \lambda_0^\tau, \dots, \lambda_r - \lambda_r^\tau\}$ of X_n^- with $\ell = \lambda_r \lambda_r^\tau$, and an oriented basis $\{\epsilon_0, \dots, \epsilon_r\}$ of $(1-\tau)\mathcal{E}_n$ as in Lemma 8.1, so that $\{\epsilon_0, \dots, \epsilon_{r-1}\}$ is an oriented basis of $(1-\tau)\mathcal{E}_{n/\ell}$. Then

$$(R_n)_{\ell,f} = \begin{vmatrix} (\epsilon_0)_{\ell,\mathrm{f}} & \cdots & (\epsilon_{r-1})_{\ell,\mathrm{f}} & (\epsilon_r)_{\ell,\mathrm{f}} \\ [\epsilon_0]^n_{\lambda_1} & \cdots & [\epsilon_{r-1}]^n_{\lambda_1} & [\epsilon_r]^n_{\lambda_1} \\ \vdots & & \vdots & \vdots \\ [\epsilon_0]^n_{\lambda_r} & \cdots & [\epsilon_{r-1}]^n_{\lambda_r} & [\epsilon_r]^n_{\lambda_r} \end{vmatrix}.$$

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

For each i, we have $[\epsilon_i]^n_{\lambda_r} = [\epsilon_i]^{n/\ell}_{\lambda_r} + [\epsilon_i]^{\ell}_{\lambda_r}$. If $i < r$, then ϵ_i is a unit at λ_r so $[\epsilon_i]^{n/\ell}_{\lambda_r} = 0$. Thus

$$(R_n)_{\ell,f} = \begin{vmatrix} (\epsilon_0)_{\ell,\mathrm{f}} & \cdots & (\epsilon_r)_{\ell,\mathrm{f}} \\ [\epsilon_0]^n_{\lambda_1} & \cdots & [\epsilon_r]^n_{\lambda_1} \\ \vdots & & \vdots \\ [\epsilon_0]^{\ell}_{\lambda_r} & \cdots & [\epsilon_r]^{\ell}_{\lambda_r} \end{vmatrix} + \begin{vmatrix} (\epsilon_0)_{\ell,\mathrm{f}} & \cdots & (\epsilon_{r-1})_{\ell,\mathrm{f}} & (\epsilon_r)_{\ell,\mathrm{f}} \\ [\epsilon_0]^n_{\lambda_1} & \cdots & [\epsilon_{r-1}]^n_{\lambda_1} & [\epsilon_r]^n_{\lambda_1} \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & [\epsilon_r]^{n/\ell}_{\lambda_r} \end{vmatrix}.$$

The map $\epsilon \mapsto [\epsilon]^{\ell}_{\lambda_r} = [\epsilon, F_{\lambda_r}(\boldsymbol{\mu}_\ell)/F_{\lambda_r}] - 1$ is an isomorphism from $(\hat{F}^\times_{\ell,\mathrm{f}})^- = (\hat{\mathcal{O}}^\times_\ell)^-$ to $(I_\ell/I_\ell^2) \otimes \mathbb{Z}_p$, and is zero on $(\hat{F}^\times_{\ell,\mathrm{tr}})^-$ because ℓ is a norm in the extension $F_{\lambda_r}(\boldsymbol{\mu}_\ell)/F_{\lambda_r} = \mathbb{Q}_\ell(\boldsymbol{\mu}_\ell)/\mathbb{Q}_\ell$. Hence the first determinant in the equation above is zero, because the top and bottom rows are linearly dependent. Also, if $i < r$ then ϵ_i is a unit at λ_r, so $(\epsilon_i)_{\ell,\mathrm{f}} = (\epsilon_i)_\ell$ and

$$(R_n)_{\ell,\mathrm{f}} = \begin{vmatrix} (\epsilon_0)_\ell & \cdots & (\epsilon_{r-1})_\ell \\ [\epsilon_0]^n_{\lambda_1} & \cdots & [\epsilon_{r-1}]^n_{\lambda_1} \\ \vdots & & \vdots \\ [\epsilon_0]^n_{\lambda_{r-1}} & \cdots & [\epsilon_{r-1}]^n_{\lambda_{r-1}} \end{vmatrix} [\epsilon_r]^{n/\ell}_{\lambda_r} = (S_{n/\ell,n})_\ell \, [\epsilon_r]^{n/\ell}_{\lambda_r}.$$

By Lemma 8.1, $[\epsilon_r]^{n/\ell}_{\lambda_r} = -(h_{n/\ell}/h_n)\, \pi_{n/\ell}(\mathrm{Fr}_\ell - 1)$. Thus

$$h_n \langle (R_n)_{\ell,\mathrm{f}} \rangle^{\mathrm{new}}_n = -h_{n/\ell} \langle (S_{n/\ell,n})_\ell \, \pi_{n/\ell}(\mathrm{Fr}_\ell - 1) \rangle^{\mathrm{new}}_n. \tag{10}$$

We can now 'simplify' (10) by inductively expanding the right-hand side using Proposition 8.5. Specifically, expand $\langle S_{n/\ell,n}\, \pi_{n/\ell}(\mathrm{Fr}_\ell - 1)\rangle^{\mathrm{new}}_n$ using Proposition 8.5(ii). Then expand each of the resulting $\langle S_{n/(\ell q),n/\ell}\, \pi_{n/(q\ell)}(\mathrm{Fr}_q - 1)\rangle^{\mathrm{new}}_{n/\ell}$ using Proposition 8.5(ii) again. Continue until no terms $S_{m/q,m}$ remain. The resulting sum consists of one term

$$(-1)^k \langle h_{n/(q_1\cdots q_k)}(R_{n/(q_1\cdots q_k)})_\ell \rangle^{\mathrm{new}}_{n/(q_1\cdots q_k)} \prod_{i=1}^{k} \pi_{q_i}(\mathrm{Fr}_{q_{i+1}} - 1)$$

for each sequence $q_1 = \ell, q_2, \ldots, q_k$ of distinct primes dividing n_+ (with $q_{k+1} = \ell$). Identifying this sequence with the k-cycle $\sigma := (\ell, q_2, \ldots, q_k) \in \mathfrak{S}_1(n)$ gives the formula of the theorem, since $\mathrm{sign}(\sigma) = (-1)^{k-1}$. □

Theorem 8.7. *The collection $\{h_n R_n : n \in \mathcal{N}_p\}$ is a pre-Kolyvagin system.*

Proof. We need to check the five properties of Definition 6.2. Property (i) is Lemma 8.3, (ii) is Proposition 8.2, (iii) is Proposition 8.4, (iv) is Theorem 8.6 along with Remark 6.9, and (v) is Proposition 8.5(i). □

9. Proof of Theorem 3.9

Proof of Theorem 3.9. Fix an odd prime p. By Theorems 7.2 and 8.7, we have pre-Kolyvagin systems

$$\{2^{-s(n)}\tilde{\theta}_n : n \in \mathcal{N}_p\}, \quad \{-h_n R_n : n \in \mathcal{N}_p\}.$$

By Proposition 3.10, $\tilde{\theta}'_1 = -h_1 R_1$ in $\mathcal{O}_F^\times/\{\pm 1\}$. Hence, by Corollary 6.6,

$$2^{-s(n)}\tilde{\theta}_n = -h_n R_n \quad \text{in } (F^\times)^- \otimes \mathcal{I}_n^{\mathrm{new}} \otimes \mathbb{Z}_p \text{ for every } n \in \mathcal{N}_p. \tag{11}$$

If $p | n \in \mathcal{N}$, then Proposition 4.2(iv) shows that $(p-1)\mathcal{I}_n^{\mathrm{new}} = 0$. Therefore $(F^\times)^- \otimes \mathcal{I}_n^{\mathrm{new}} \otimes \mathbb{Z}_p = 0$ and (11) holds vacuously in this case. Since (11) holds for every $n \in \mathcal{N}$ and every odd prime p, this completes the proof of Theorem 3.9. □

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press

References

Dar95 H. Darmon, *Thaine's method for circular units and a conjecture of Gross*, Canad. J. Math. **47** (1995), 302–317.

Gro88 B. Gross, *On the values of abelian L-functions at $s = 0$*, J. Fac. Sci. Univ. Tokyo **35** (1988), 177–197.

Hal85 A. Hales, *Stable augmentation quotients of abelian groups*, Pacific J. Math. **118** (1985), 401–410.

Hay88 D. Hayes, *The refined $\mathfrak{p}$-adic abelian Stark conjecture in function fields*, Invent. Math. **94** (1988), 505–527.

MR04a B. Mazur and K. Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **799** (2004).

MR04b B. Mazur and K. Rubin, *Introduction to Kolyvagin systems*, in *Stark's conjectures: recent work and new directions*, Contemporary Mathematics, vol. 358 (American Mathematical Society, Providence, RI, 2004), 207–221.

MT87 B. Mazur and J. Tate, *Refined conjectures of the 'Birch and Swinnerton–Dyer type'*, Duke Math. J. **54** (1987), 711–750.

Rub96 K. Rubin, *A Stark conjecture 'over $\mathbb{Z}$' for abelian L-functions with multiple zeros*, Ann. Inst. Fourier (Grenoble) **46** (1996), 33–62.

Rub00 K. Rubin, *Euler systems*, Annals of Mathematics Studies, vol. 147 (Princeton University Press, Princeton, NJ, 2000).

Sta80 H. Stark, *L-functions at $s = 1$. IV. First derivatives at $s = 0$*, Adv. Math. **35** (1980), 197–235.

Barry Mazur mazur@math.harvard.edu
Department of Mathematics, Harvard University, Cambridge, MA 02138, USA

Karl Rubin krubin@math.uci.edu
Department of Mathematics, UC Irvine, Irvine, CA 92697, USA

https://doi.org/10.1112/S0010437X1000494X Published online by Cambridge University Press