Proceedings of the International Congress of Mathematicians
Hyderabad, India, 2010

Selmer Groups and Congruences

Ralph Greenberg[*]

Abstract

We first introduce Selmer groups for elliptic curves, and then Selmer groups for Galois representations. The main topic of the article concerns the behavior of Selmer groups for Galois representations with the same residual representation. We describe a variety of situations where this behavior can be studied fruitfully.

Mathematics Subject Classification (2010). Primary 11G05, 11R23; Secondary 11G40, 11R34.

Keywords. Selmer groups, Iwasawa invariants, Root numbers, Parity conjecture,

1. Selmer Groups

Suppose that E is an elliptic curve defined over a number field F. Let $E(F)$ denote the set of points on E defined over F. Under a certain simply-defined operation, $E(F)$ becomes an abelian group. The classical Mordell-Weil theorem asserts that $E(F)$ is finitely-generated. One crucial step in proving this theorem is to show that $E(F)/nE(F)$ is a finite group for some integer $n \geq 2$. In essence, one proves this finiteness for any n by defining a map from $E(F)/nE(F)$ to the Selmer group for E over F and showing that the kernel and the image of that map are finite.

We will regard F as a subfield of $\overline{\mathbf{Q}}$, a fixed algebraic closure of $\mathbf{Q}$. The torsion subgroup E_{tors} of $E(\overline{\mathbf{Q}})$ is isomorphic to $(\mathbf{Q}/\mathbf{Z})^2$ as a group. One has a natural action of $\mathrm{G}_F = \mathrm{Gal}(\overline{\mathbf{Q}}/F)$ on E_{tors}. The Selmer group is a certain subgroup of the Galois cohomology group $H^1(\mathrm{G}_F, E_{tors})$. Its definition involves Kummer theory for E and is based on the fact that the group of points on E defined over any algebraically closed field is a divisible group.

As is customary, we will write $H^1(F, E_{tors})$ instead of $H^1(\mathrm{G}_F, E_{tors})$. A similar abbreviation will be used for other Galois cohomology groups. Suppose

[*]The author's research described in this article has been supported by grants from the National Science Foundation.

Department of Mathematics, University of Washington, Seattle, WA 98195-4350, USA.
E-mail: greenber@math.washington.edu.

that $P \in E(F)$ and that $n \geq 1$. Then there exists a point $Q \in E(\overline{\mathbf{Q}})$ such that $nQ = P$. In fact, there are n^2 such points Q, all differing by points in E_{tors} of order dividing n. If $g \in \mathrm{G}_F$ and $Q' = g(Q)$, then $nQ' = P$. Therefore, we have $g(Q) - Q \in E_{tors}$. The map $\varphi : G_F \to E_{tors}$ defined by $\varphi(g) = g(Q) - Q$ is a 1-cocycle and defines a class $[\varphi]$ in $H^1(F, E_{tors})$. In this way, we can define the *"Kummer map"*

$$\kappa : \; E(F) \otimes_{\mathbf{Z}} (\mathbf{Q}/\mathbf{Z}) \;\longrightarrow\; H^1(F, E_{tors}).$$

The image of $P \otimes \big(\frac{1}{n} + \mathbf{Z}\big)$ is defined to be the class $[\varphi]$. The map κ is an injective homomorphism.

If v is any prime of F, we can similarly define the v-adic Kummer map

$$\kappa_v : \; E(F_v) \otimes_{\mathbf{Z}} (\mathbf{Q}/\mathbf{Z}) \;\longrightarrow\; H^1(F_v, E_{tors}),$$

where F_v is the completion of F at v. One can identify G_{F_v} with a subgroup of G_F by choosing an embedding of $\overline{\mathbf{Q}}$ into an algebraic closure of F_v which extends the embedding of F into F_v, and thereby define a restriction map from $H^1(F, E_{tors})$ to $H^1(F_v, E_{tors})$. One has such a map for each prime v of F, even for the archimedean primes. One then defines the Selmer group $\mathrm{Sel}_E(F)$ to be the kernel of the map

$$\sigma : \; H^1(F, E_{tors}) \;\longrightarrow\; \bigoplus_v H^1(F_v, E_{tors})\big/\mathrm{im}(\kappa_v),$$

where v runs over all the primes of F. One shows that the image of σ is actually contained in the direct sum and that this definition of $\mathrm{Sel}_E(F)$ does not depend on the choice of embeddings. The image of the Kummer map κ is clearly a subgroup of $\mathrm{Sel}_E(F)$. The corresponding quotient group $\mathrm{Sel}_E(F)\big/\mathrm{im}(\kappa)$ is the Tate-Shafarevich group for E over F.

The elliptic curve E is determined up to isomorphism over F by the action of G_F on E_{tors}. This result was originally conjectured by Tate and proved by Faltings [10]. If p is a prime and $n \geq 1$, then the p^n-torsion on E will be denoted by $E[p^n]$. The p-primary subgroup of E_{tors} is the union of the groups $E[p^n]$ and will be denoted by $E[p^\infty]$. The inverse limit of the $E[p^n]$'s is the p-adic Tate module $T_p(E)$. It is a free $\mathbf{Z}_p$-module of rank 2, where $\mathbf{Z}_p$ denotes the ring of p-adic integers. All of these objects have a continuous action of G_F. We let $V_p(E) = T_p(E) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, a 2-dimensional representation space for G_F over $\mathbf{Q}_p$, the field of p-adic numbers. Faltings proves the following version of Tate's conjecture: The elliptic curve E is determined up to isogeny over F by the isomorphism class of the representation space $V_p(E)$ for G_F. The Tate module $T_p(E)$ determines E up to an isogeny of degree prime to p.

The above theorem of Faltings suggests that arithmetic properties of E which depend only on the isomorphism class of E over F should somehow be determined by the Galois module E_{tors}. In particular, the structure of $E(F)$

should be so determined. It is clear how to determine the torsion subgroup of $E(F)$ in terms of E_{tors}. It is just $H^0(F, E_{tors})$. Now it is conjectured that the Tate-Shafarevich group for an elliptic curve over a number field is always finite. If this is so, then the image of the Kummer map should be precisely the maximal divisible subgroup $\mathrm{Sel}_E(F)_{div}$ of $\mathrm{Sel}_E(F)$. If r is the rank of $E(F)$, then that image is isomorphic to $(\mathbf{Q}/\mathbf{Z})^r$. Thus, at least conjecturally, one can determine r from the structure of $\mathrm{Sel}_E(F)$. And, as we will now explain, one can describe $\mathrm{Sel}_E(F)$ entirely in terms of the Galois module E_{tors}. This is not immediately apparent from the definition given earlier.

Let p be any prime. The p-primary subgroup $\mathrm{Sel}_E(F)_p$ of $\mathrm{Sel}_E(F)$ is a subgroup of $H^1(F, E[p^\infty])$. It can be defined as the kernel of the map

$$\sigma_p : \ H^1(F, E[p^\infty]) \ \longrightarrow \ \bigoplus_v H^1(F_v, E[p^\infty])/\mathrm{im}(\kappa_{v,p}) \ \ ,$$

where $\kappa_{v,p}$ is the restriction of κ_v to the p-primary subgroup of $E(F_v)\otimes_{\mathbf{Z}}(\mathbf{Q}/\mathbf{Z})$. Thus, if we can describe the image of $\kappa_{v,p}$ for all primes v of F just in terms of the Galois module $E[p^\infty]$, then we will have such a description of $\mathrm{Sel}_E(F)_p$.

First of all, suppose that v is a nonarchimedean prime and that the residue field for v has characteristic ℓ, where $\ell \neq p$. It is known that $E(F_v)$ is an ℓ-adic Lie group. More precisely, $E(F_v)$ contains a subgroup of finite index which is isomorphic to $\mathbf{Z}_\ell^{[F_v:\mathbf{Q}_\ell]}$. Since that group is divisible by p, one sees easily that $E(F_v) \otimes_{\mathbf{Z}} (\mathbf{Q}_p/\mathbf{Z}_p)$, the p-primary subgroup of $E(F_v) \otimes_{\mathbf{Z}} (\mathbf{Q}/\mathbf{Z})$, actually vanishes. Hence $\mathrm{im}(\kappa_{v,p}) = 0$ if $v \nmid p$. A similar argument shows that the same statement is true if v is archimedean.

Now assume that the residue field for v has characteristic p. We also assume that E has good ordinary reduction at v. Good reduction means that one can find an equation for E over the ring of integers of F such that its reduction modulo v defines an elliptic curve $\overline{E}_v$ over the residue field $\mathbf{F}_v$. The reduction is ordinary if the integer $a_v = 1+|\mathbf{F}_v|-|\overline{E}_v(\mathbf{F}_v)|$ is not divisible by p. Equivalently, ordinary reduction means that $\overline{E}_v[p^\infty]$ is isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$ as a group. Reduction modulo v then defines a surjective homomorphism from $E[p^\infty]$ to $\overline{E}_v[p^\infty]$. Its kernel turns out to be the group of p-power torsion points on a formal group. We denote that kernel by C_v. It is invariant under the action of G_{F_v} and is isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$ as a group. We have $E[p^\infty]/C_v \cong \overline{E}_v[p^\infty]$. Remarkably, one has the following description of the image of $\kappa_{v,p}$:

$$\mathrm{im}(\kappa_{v,p}) \ = \ \mathrm{im}\big(H^1(F_v, C_v)_{div} \ \longrightarrow \ H^1(F_v, E[p^\infty])\big).$$

One can characterize C_v as follows: It is a G_{F_v}-invariant subgroup of $E[p^\infty]$ and $E[p^\infty]/C_v$ is the maximal quotient of $E[p^\infty]$ which is unramified for the action of G_{F_v}. Thus, the above description of $\mathrm{im}(\kappa_{v,p})$ just involves the Galois module $E[p^\infty]$, as we wanted.

The above description of $\mathrm{im}(\kappa_{v,p})$ was given in [4]. The argument is not very difficult. If E does not have good ordinary reduction at v, there is still a description of $\mathrm{im}(\kappa_{v,p})$ in terms of $E[p^\infty]$. This was given by Bloch and Kato in [2]. It involves Fontaine's ring B_{crys}. One defines the subspace $H^1_f\big(F_v, V_p(E)\big)$ of $H^1\big(F_v, V_p(E)\big)$ to be the kernel of the the natural map from $H^1\big(F_v, V_p(E)\big)$ to $H^1\big(F_v, V_p(E) \otimes_{\mathbf{Q}_p} B_{crys}\big)$. One has $V_p(E)/T_p(E) \cong E[p^\infty]$. Then $\mathrm{im}(\kappa_{v,p})$ turns out to be the image of $H^1_f\big(F_v, V_p(E)\big)$ under the natural map from $H^1\big(F_v, V_p(E)\big)$ to $H^1(F_v, E[p^\infty])$.

The fact that $\mathrm{Sel}_E(F)_p$ can be defined solely in terms of the Galois module $E[p^\infty]$ was a valuable insight in the 1980's. It suggested a way to give a reasonable definition of Selmer groups in a far more general context. This idea was pursued in [11] for the purpose of generalizing conjectures of Iwasawa and of Mazur concerning the algebraic interpretation of zeros of p-adic L-functions. It was also pursued by Bloch and Kato in [2] for the purpose of generalizing the Birch and Swinnerton-Dyer conjecture.

Since $\mathrm{Sel}_E(F)_p$ is determined by the Galois module $E[p^\infty]$, one can ask whether $\mathrm{Sel}_E(F)[p]$ is determined by the Galois module $E[p]$. This turns out not to be so. Suppose that E_1 and E_2 are elliptic curves defined over F and that $E_1[p] \cong E_2[p]$ as G_F-modules. It is quite possible for $\mathrm{Sel}_{E_1}(F)[p]$ and $\mathrm{Sel}_{E_2}(F)[p]$ to have different $\mathbf{F}_p$-dimensions. In the next section of this article, we will consider this question in the setting of Iwasawa theory. Thus, we will consider the Selmer group for an elliptic curve E over a certain infinite extension F_∞ of F, the so-called *"cyclotomic $\mathbf{Z}_p$-extension"* of F.

Let μ_{p^∞} denote the group of p-power roots of unity in $\overline{\mathbf{Q}}$. Then F_∞ is the unique subfield of $F(\mu_{p^\infty})$ such that $\mathrm{Gal}(F_\infty/F) \cong \mathbf{Z}_p$. We denote that Galois group by Γ. For each $n \geq 0$, Γ has a unique subgroup Γ_n of index p^n. Thus, $F_n = F_\infty^{\Gamma_n}$ is a cyclic extension of F of degree p^n. One can define the Selmer group for E over F_∞ to be the direct limit of the Selmer groups $\mathrm{Sel}_E(F_n)$ as $n \to \infty$. We will concentrate on its p-primary subgroup $\mathrm{Sel}_E(F_\infty)_p$. Now Γ acts naturally on $\mathrm{Sel}_E(F_\infty)_p$. Regarding $\mathrm{Sel}_E(F_\infty)_p$ as a discrete $\mathbf{Z}_p$-module, the action of Γ is continuous and $\mathbf{Z}_p$-linear. We can then regard $\mathrm{Sel}_E(F_\infty)_p$ as a discrete Λ-module, where $\Lambda = \mathbf{Z}_p[[\Gamma]]$ is the completed $\mathbf{Z}_p$-group algebra for the pro-p group Γ. That is, Λ is the inverse limit of the $\mathbf{Z}_p$-group algebras $\mathbf{Z}_p[\Gamma_n]$ defined by the obvious surjective $\mathbf{Z}_p$-algebra homomorphisms $\mathbf{Z}_p[\Gamma_m] \to \mathbf{Z}_p[\Gamma_n]$ for $m \geq n \geq 0$. One often refers to Λ as the *"Iwasawa algebra"* for Γ (over $\mathbf{Z}_p$). A very useful fact in Iwasawa theory is that Λ is isomorphic (non-canonically) to the formal power series ring $\mathbf{Z}_p[[T]]$ in one variable. Thus, Λ is a complete Noetherian local ring of Krull dimension 2.

Assuming that E has good ordinary reduction at the primes of F lying over p, one has a description of $\mathrm{Sel}_E(F_\infty)_p$ just as above. If v is a prime of F not dividing p, and η is a prime of F_∞ lying over v, then the image of the Kummer map over $F_{\infty,\eta}$ is again trivial. If $v|p$, then the direct limits of the local Galois cohomology groups $H^1(F_{n,\eta}, C_\eta)_{div}$ and $H^1(F_{n,\eta}, C_\eta)$ as $n \to \infty$ turn out to be the same, both equal to $H^1(F_{\infty,\eta}, C_\eta)$. Thus, the image of the Kummer map over $F_{\infty,\eta}$ coincides with the image of the map

$$\varepsilon_{\infty,\eta} : H^1(F_{\infty,\eta}, C_\eta) \longrightarrow H^1(F_{\infty,\eta}, E[p^\infty]) \quad .$$

A very broad generalization of this fact is proven in [4].

The following conjecture of Mazur will play a fundamental role in most of the results we will describe. It was first stated and discussed in [21]. We let $X_E(F_\infty)$ denote the Pontryagin dual of $\mathrm{Sel}_E(F_\infty)_p$. We can regard $X_E(F_\infty)$ as a compact Λ-module. It turns out to always be finitely-generated as a Λ-module. As in [21], we will say that $\mathrm{Sel}_E(F_\infty)_p$ is a cotorsion Λ-module if $X_E(F_\infty)$ is a torsion Λ-module.

Conjecture. *Suppose that E has good ordinary reduction at the primes of F lying over p. Then $\mathrm{Sel}_E(F_\infty)_p$ is a cotorsion Λ-module.*

The above conjecture is proved in [21] under the assumption that $\mathrm{Sel}_E(F)_p$ is finite. We will later cite a much more recent theorem (due to Kato and Rohrlich) which asserts that $\mathrm{Sel}_E(F_\infty)_p$ is indeed Λ-cotorsion if E is an elliptic curve defined over $\mathbf{Q}$ with good ordinary reduction at p and F is any abelian extension of $\mathbf{Q}$. Such a theorem had already been proven by Rubin [31] in the case where E has complex multiplication.

The above conjecture should be valid under somewhat weaker assumptions about the reduction of E at the primes above p. It should suffice to just assume that E does not have potentially supersingular reduction at any of those primes. That assumption is necessary. If E has potentially supersingular reduction at a prime above p, then one can show that $\mathrm{Sel}_E(F_\infty)_p$ is not Λ-cotorsion. We refer the reader to [34] for a discussion of this issue and a precise conjecture about the rank of $X_E(F_\infty)$ as a Λ-module.

2. Behavior Under Congruences

The results that we describe here are mostly from [14]. We will now take $F = \mathbf{Q}$, partly just to simplify the discussion and partly because the deep theorem of Kato and Rohrlich mentioned above is then available. We will also assume that p is an odd prime. We concentrate entirely on the p-primary subgroup of Selmer groups. Let $\mathbf{Q}_\infty$ denote the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. Suppose that E is defined over $\mathbf{Q}$ and has good ordinary reduction at p.

Let π denote the unique prime of $\mathbf{Q}_\infty$ lying over p. We will write $\overline{E}$ for $\overline{E}_p$. It will be useful to note that the image of $\varepsilon_{\infty,\pi}$ coincides with the kernel of the map $H^1(\mathbf{Q}_{\infty,\pi}, E[p^\infty]) \to H^1(\mathbf{Q}_{\infty,\pi}, \overline{E}[p^\infty])$. That map turns out to be surjective and so $H^1(\mathbf{Q}_{\infty,\pi}, E[p^\infty])/\mathrm{im}(\varepsilon_{\infty,\pi})$ is isomorphic to $H^1(\mathbf{Q}_{\infty,\pi}, \overline{E}[p^\infty])$, which we will denote by $\mathcal{H}_p(\mathbf{Q}_\infty, E[p^\infty])$. We will denote $H^1(\mathbf{Q}_{\infty,\pi}, \overline{E}[p])$ by $\mathcal{H}_p(\mathbf{Q}_\infty, E[p])$.

If ℓ is a non-archimedean prime, and $\ell \neq p$, we define

$$\mathcal{H}_\ell(\mathbf{Q}_\infty, E[p^\infty]) \;=\; \bigoplus_{\eta|\ell} H^1(\mathbf{Q}_{\infty,\eta}, E[p^\infty]),$$

a finite direct sum because ℓ is finitely decomposed in $\mathbf{Q}_\infty/\mathbf{Q}$. We similarly define $\mathcal{H}_\ell(\mathbf{Q}_\infty, E[p])$, just replacing the Galois module $E[p^\infty]$ by $E[p]$. We will ignore the local Galois cohomology groups for archimedean primes. They are trivial since we are assuming that p is odd.

Although the Galois module $E[p]$ still does not determine $\mathrm{Sel}_E(F_\infty)[p]$, a somewhat weaker statement turns out to be true. To formulate it, we introduce *"non-primitive"* Selmer groups. Suppose that Σ_0 is a finite set of non-archimedean primes of $\mathbf{Q}$. We assume that $p \notin \Sigma_0$. The corresponding non-primitive Selmer group will be denoted by $\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)_p$ and differs from the actual Selmer group in that we omit the local conditions for the primes of $\mathbf{Q}_\infty$ lying above primes in Σ_0. To be precise, $\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)_p$ is defined to be the kernel of the following map:

$$H^1(\mathbf{Q}_\infty, E[p^\infty]) \;\longrightarrow\; \bigoplus_{\ell \notin \Sigma_0} \mathcal{H}_\ell(\mathbf{Q}_\infty, E[p^\infty]). \tag{1}$$

If we take Σ_0 to be empty, then $\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)_p = \mathrm{Sel}_E(\mathbf{Q}_\infty)_p$.

Suppose that $E[p]$ is irreducible and that Σ_0 contains the primes where E has bad reduction. The map $H^1(\mathbf{Q}_\infty, E[p]) \to H^1(\mathbf{Q}_\infty, E[p^\infty])[p]$ is an isomorphism. The role of the assumption about Σ_0 is that it implies that the preimage of $\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)[p]$ under that isomorphism is precisely the kernel of the map

$$H^1(\mathbf{Q}_\infty, E[p]) \longrightarrow \bigoplus_{\ell \notin \Sigma_0} \mathcal{H}_\ell(\mathbf{Q}_\infty, E[p]). \tag{2}$$

Note that the groups and maps here indeed depend only on the Galois module $E[p]$. This is clear for $\ell \neq p$. For $\ell = p$, it follows because one can characterize $\overline{E}[p]$ as the maximal unramified quotient of $E[p]$ for the action of $G_{\mathbf{Q}_p}$. This is so because p is assumed to be odd and therefore the action of the inertia subgroup of $G_{\mathbf{Q}_p}$ on the kernel of the reduction map $E[p] \to \overline{E}[p]$ is nontrivial. Thus, under the above assumption about Σ_0, we have a description of $\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)[p]$ in terms of the Galois module $E[p]$.

The local Galois cohomology groups $\mathcal{H}_\ell(\mathbf{Q}_\infty, E[p^\infty])$ can be studied by using standard results, essentially just local class field theory. One finds that

$$\mathcal{H}_\ell(\mathbf{Q}_\infty, E[p^\infty]) \cong (\mathbf{Q}_p/\mathbf{Z}_p)^{\delta(E,\ell)}$$

for any prime $\ell \neq p$, where $\delta(E,\ell)$ is an easily determined non-negative integer.

A theorem of Kato [18], combined with a theorem of Rohrlich [29], implies that $\mathrm{Sel}_E(\mathbf{Q}_\infty)_{p,div} \cong (\mathbf{Q}_p/\mathbf{Z}_p)^{\lambda(E)}$ for some integer $\lambda(E) \geq 0$. This means that the Pontryagin dual of $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$ is a torsion module over the Iwasawa algebra $\Lambda = \mathbf{Z}_p[[\Gamma]]$. This was conjectured to be so in [21], as we mentioned in section 1. The integer $\lambda(E)$ is the $\mathbf{Z}_p$-corank of $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$. Under the assumption that $E[p]$ is irreducible as a Galois module, it is reasonable to make the conjecture that the Pontryagin dual of $\mathrm{Sel}_E(\mathbf{Q}_\infty)[p]$ is a torsion module over $\Lambda/p\Lambda$. Equivalently, this would mean that $\mathrm{Sel}_E(\mathbf{Q}_\infty)[p]$ is finite, and hence that the so-called μ-invariant for $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$ vanishes. If so, then one can prove that $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$ is a divisible group and so one would have an isomorphism

$$\mathrm{Sel}_E(\mathbf{Q}_\infty)_p \;\cong\; (\mathbf{Q}_p/\mathbf{Z}_p)^{\lambda(E)}.$$

The fact that $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$ is a cotorsion Λ-module allows one to prove that the map

$$\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)_p \;\longrightarrow\; \bigoplus_{\ell\in\Sigma_0} \mathcal{H}_\ell(\mathbf{Q}_\infty, E[p^\infty])$$

is surjective. The kernel of that map is $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$, and so we have an isomorphism

$$\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)_p/\mathrm{Sel}_E(\mathbf{Q}_\infty)_p \;\cong\; \bigoplus_{\ell\in\Sigma_0} \mathcal{H}_\ell(\mathbf{Q}_\infty, E[p^\infty]) \;\cong\; (\mathbf{Q}_p/\mathbf{Z}_p)^{\delta(E,\Sigma_0)} \quad ,$$

where $\delta(E,\Sigma_0) = \sum_{\ell\in\Sigma_0}\delta(E,\ell)$. Let $\lambda(E,\Sigma_0)$ denote the $\mathbf{Z}_p$-corank of $\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)_p$. We then obtain the formula $\lambda(E,\Sigma_0) = \lambda(E) + \delta(E,\Sigma_0)$.

If $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$ is divisible, then it is a direct summand in $\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)_p$, and so we will have

$$\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty) \;\cong\; \mathrm{Sel}_E(\mathbf{Q}_\infty) \;\oplus\; \left(\bigoplus_{\ell\in\Sigma_0} \mathcal{H}_\ell(\mathbf{Q}_\infty, E[p^\infty])\right).$$

Thus, $\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)_p$ will also be divisible, and so its $\mathbf{Z}_p$-corank $\lambda(E,\Sigma_0)$ will be equal to the $\mathbf{F}_p$-dimension of $\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)[p]$. A similar statement is true for all of the summands in the above direct sum.

Suppose that E_1 and E_2 are elliptic curves defined over $\mathbf{Q}$, that both have good ordinary reduction at p, and that $E_1[p] \cong E_2[p]$ as $\mathrm{G}_{\mathbf{Q}}$-modules. We think of such an isomorphism as a congruence modulo p between the p-adic Tate modules for E_1 and E_2. We will also assume that $G_{\mathbf{Q}}$ acts irreducibly on $E_1[p]$, and hence on $E_2[p]$. Suppose that Σ_0 is chosen to include all the primes where E_1 or E_2 have bad reduction. Under these assumptions, the above discussion shows that

$$\mathrm{Sel}_{E_1}^{\Sigma_0}(\mathbf{Q}_\infty)[p] \;\cong\; \mathrm{Sel}_{E_2}^{\Sigma_0}(\mathbf{Q}_\infty)[p].$$

Consequently, if $\mathrm{Sel}_{E_1}(\mathbf{Q}_\infty)[p]$ is finite, then so is $\mathrm{Sel}_{E_2}(\mathbf{Q}_\infty)[p]$. Their $\mathbf{F}_p$-dimensions will be equal and one then obtains the formula

$$\lambda(E_1) + \delta(E_1,\Sigma_0) \;=\; \lambda(E_2) + \delta(E_2,\Sigma_0) \quad .$$

Since the quantities $\delta(E_1, \Sigma_0)$ and $\delta(E_2, \Sigma_0)$ can be evaluated, one can then determine $\lambda(E_2)$ if one knows $\lambda(E_1)$.

As an example, consider the two elliptic curves

$$E_1 : y^2 = x^3 + x - 10, \qquad E_2 : y^2 = x^3 - 584x + 5444$$

which have conductors 52 and $364 = 7 \cdot 52$, respectively. We take $p = 5$ and $\Sigma_0 = \{2, 7, 13\}$. One has a congruence modulo 5 between the q-expansions of the modular forms corresponding to E_1 and E_2, ignoring the terms for powers q^n where $7|n$. It follows that $E_1[5] \cong E_2[5]$ as $G_{\mathbf{Q}}$-modules. It turns out that $\mathrm{Sel}_{E_1}(\mathbf{Q}_\infty)_p = 0$. Hence, one has $\lambda(E_1) = 0$. One finds that $\delta(E_1, \Sigma_0) = 5$ and $\delta(E_2, \Sigma_0) = 0$. Consequently, we have $\lambda(E_2) = 5$.

Such isomorphisms $E_1[p] \cong E_2[p]$ are not hard to find for $p = 3$ and $p = 5$. In fact, it is shown in [33] that for $p \leq 5$, and for a fixed elliptic curve E_1 defined over $\mathbf{Q}$, one can explicitly describe equations defining an infinite family of non-isomorphic elliptic curves E_2 over $\mathbf{Q}$ with $E_2[p] \cong E_1[p]$. Such isomorphisms are not common for $p \geq 7$. However, if one considers cusp forms of weight 2, then *"raising the level"* theorems show that such isomorphisms occur for every odd prime p. They can be formulated in terms of the Jacobian variety attached to Hecke eigenforms of weight 2. An isomorphism amounts to a congruence between the q-expansions of two such eigenforms. The results described above extend without any real difficulty to this case.

A somewhat different approach is taken in [9]. That paper considers Selmer groups over $\mathbf{Q}_\infty$ associated to Hecke eigenforms of arbitrary weight which are ordinary in a certain sense. If one fixes the residual representation and bounds the prime-to-p part of the conductor, then such eigenforms occur in Hida families which are parametrized by the set of prime ideals of height 1 in a certain ring R. Such families were constructed by Hida in [17]. If $\mathfrak{a}$ is a minimal prime ideal of R, then the height 1 prime ideals of $R/\mathfrak{a}$ parametrize one *"branch"* in such a family. For each eigenform h, one can associate a Galois representation V_h of dimension 2 over a field $\mathcal{F}$, a finite extension of $\mathbf{Q}_p$. Let $\mathcal{O}$ be the ring of integers in $\mathcal{F}$ and let π be a uniformizing parameter. Let $\mathfrak{f} = \mathcal{O}/(\pi)$. One can choose a Galois-invariant $\mathcal{O}$-lattice T_h in V_h and then define a discrete Galois module $\mathcal{A}_h = V_h/T_h$. The representation is ordinary in the sense that V_h has a 1-dimensional quotient which is unramified for the action of $\mathrm{G}_{\mathbf{Q}_p}$. Hence $\mathcal{A}_h$ has an unramified quotient which has $\mathcal{O}$-corank 1.

One can define a Selmer group $\mathrm{Sel}_{\mathcal{A}_h}(\mathbf{Q}_\infty)_p$ for the Galois module $\mathcal{A}_h$ in essentially the same way as for $E[p^\infty] = V_p(E)/T_p(E)$. It is a subgroup of $H^1(\mathbf{Q}_\infty, \mathcal{A}_h)$ and is defined as the kernel of a map just like (1) (taking Σ_0 to be empty). It suffices to define $\mathcal{H}_\ell(\mathbf{Q}_\infty, \mathcal{A}_h)$ for all primes ℓ. The residual representation is given by the Galois action on $\mathcal{A}_h[\pi]$. If we assume that this is irreducible, as before, then $H^0(\mathbf{Q}_\infty, \mathcal{A}_h) = 0$ and one has an isomorphism

$$H^1(\mathbf{Q}_\infty, \mathcal{A}_h[\pi]) \longrightarrow H^1(\mathbf{Q}_\infty, \mathcal{A}_h)[\pi]. \tag{3}$$

The preimage of $\mathrm{Sel}_{\mathcal{A}_h}(\mathbf{Q}_\infty)[\pi]$ under this isomorphism defines an $\mathfrak{f}$-subspace $\mathcal{S}_h$ of $H^1(\mathbf{Q}_\infty, \mathcal{A}_h[\pi])$. It can be characterized by local conditions. That is, one can define $\mathcal{S}_h$ as the kernel of a map like (2) (again taking Σ_0 to be empty). However, those conditions will not generally be determined by the Galois module $\mathcal{A}_h[\pi]$.

For a prime ℓ not dividing p in some finite set Σ_0, which would usually be nonempty, and for a prime η of $\mathbf{Q}_\infty$ lying over ℓ, the map

$$H^1(\mathbf{Q}_{\infty,\eta}, \mathcal{A}_h[\pi]) \longrightarrow H^1(\mathbf{Q}_{\infty,\eta}, \mathcal{A}_h)[\pi]$$

may have a nontrivial kernel. Let $\delta_\eta(h)$ denote the $\mathfrak{f}$-dimension of the kernel. An element of $\mathcal{S}_h$ will have a trivial image in $H^1(\mathbf{Q}_{\infty,\eta}, \mathcal{A}_h)[\pi]$ (and hence satisfy the local condition for the prime η which occurs in the definition of $\mathrm{Sel}_{\mathcal{A}_h}(\mathbf{Q}_\infty)_p$), but may have a nontrivial image in $H^1(\mathbf{Q}_{\infty,\eta}, \mathcal{A}_h[\pi])$. Thus, for $\ell \in \Sigma_0$, one should define $\mathcal{H}_\ell(\mathbf{Q}_\infty, \mathcal{A}_h[\pi])$ to be a certain quotient of the direct product of the $H^1(\mathbf{Q}_{\infty,\eta}, \mathcal{A}_h[\pi])$'s for $\eta|\ell$ so that the inclusion $\mathcal{A}[\pi] \to \mathcal{A}_h$ induces an isomorphism from $\mathcal{H}_\ell(\mathbf{Q}_\infty, \mathcal{A}_h[\pi])$ to $\mathcal{H}_\ell(\mathbf{Q}_\infty, \mathcal{A}_h)[\pi]$. If one assumes that $\mathrm{Sel}_{\mathcal{A}_h}(\mathbf{Q}_\infty)[\pi]$ is finite, then it turns out that $\mathrm{Sel}_{\mathcal{A}_h}(\mathbf{Q}_\infty)$ is a divisible $\mathcal{O}$-module. Let $\lambda(h)$ denote its $\mathcal{O}$-corank. Thus, we have $\lambda(h) = \dim_{\mathfrak{f}}(\mathcal{S}_h)$. As shown in [9], the variation in $\dim_{\mathfrak{f}}(\mathcal{S}_h)$ is controlled completely by the $\delta_\eta(h)$'s. They turn out to be constant in each branch of the Hida family, and so $\lambda(h)$ will also be constant in each branch. One also obtains a rather simple formula for the change in the λ-invariant from one branch to another.

What we have described above is the algebraic side of Iwasawa theory. A substantial part of both [14] and [9] is devoted to the analytic side of Iwasawa theory, the existence and properties of p-adic L-functions. One can also associate a λ-invariant to p-adic L-functions. A natural domain of definition for those functions is $\mathrm{Hom}_{cont}(\Gamma, \overline{\mathbf{Q}}_p^\times)$. The λ-invariant is the number of zeros, counting multiplicity. In [14], a non-primitive p-adic L-function plays an important role. In both [14] and [9], the results on the algebraic and on the analytic sides are quite parallel, although the nature of the arguments is quite different. The *"main conjecture"* of Iwasawa theory for elliptic curves (due to Mazur [21]), or for modular forms (as in [11]), relates the algebraic and analytic sides in a precise way. It gives an algebraic interpretation of the zeros of the p-adic L-functions.

If E has complex multiplication, then the main conjecture has been settled by Rubin [32] in a somewhat more general situation than we are considering here. The results in [14] and in [9] together with a theorem of Kato [18] imply that if the main conjecture is valid for one elliptic curve E_1, or for one modular form h_1 in a Hida family, then, under the assumption that a certain μ-invariant vanishes, the main conjecture will also be valid for any other elliptic curve E_2 such that $E_2[p] \cong E_1[p]$, or for any other modular form h_2 in the Hida family. Thus, roughly speaking, and under suitable assumptions, the validity of the main conjecture is preserved by congruences. We also want to mention much more recent work of Skinner and Urban which may go a long way to settling this conjecture completely.

There are also results for elliptic curves with good supersingular reduction at p, and more generally for modular forms of weight 2 which are supersingular in a certain sense. This topic will be discussed in detail in [13]. The results in that paper are intended to be the analogues of those in [14], despite the fact that the corresponding Selmer groups will not be Λ-cotorsion and the corresponding p-adic L-functions will have infinitely many zeros. The higher weight case is not yet understood. One finds a discussion of that case on the analytic side in [27].

3. Artin Twists

The discussion in section 2 mostly concerns the invariant $\lambda(E)$ associated to $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$, and the non-primitive analogues $\lambda(E, \Sigma_0)$ and $\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)_p$ corresponding to a suitable set Σ_0. We will now include another variable, an Artin representation σ. We let the base field F be an arbitrary algebraic number field and denote the cyclotomic $\mathbf{Z}_p$-extension of F by F_∞. Suppose that K is a finite Galois extension of F and that $K \cap F_\infty = F$. The Artin representations to be considered will factor through $\Delta = \mathrm{Gal}(K/F)$. However, if K is allowed to vary over the finite extensions of F contained in some infinite Galois extension $\mathcal{K}$ of F satisfying $\mathcal{K} \cap F_\infty = F$, then σ can vary over all Artin representations over F which factor through $\mathrm{Gal}(\mathcal{K}/F)$. One interesting case is where $\mathrm{Gal}(\mathcal{K}/F)$ is a p-adic Lie group.

If v is a non-archimedean prime of F, let $e_v(K/F)$ denote the ramification index for v in K/F. Let

$$\Phi_{K/F} \;=\; \{v \mid v \nmid p,\ v \nmid \infty, \text{ and } e_v(K/F) \text{ is divisible by } p\ \}.$$

This finite set of primes of F will play an important role in this section. We always will assume that E has good ordinary reduction at the primes of F lying over p.

Assume that X is a free $\mathbf{Z}_p$-module of finite rank $\lambda(X)$ and that there is a $\mathbf{Z}_p$-linear action of Δ on X. Thus, X is a $\mathbf{Z}_p[\Delta]$-module. Suppose that σ is defined over $\mathcal{F}$, a finite extension of $\mathbf{Q}_p$, and that σ is absolutely irreducible. We define $\lambda(X, \sigma)$ to be the multiplicity of σ in $V_{\mathcal{F}} = X \otimes_{\mathbf{Z}_p} \mathcal{F}$, an $\mathcal{F}$-representation space for Δ of dimension $\lambda(X)$. The definition of $\lambda(X, \sigma)$ makes sense if we just assume that X/X_{tors} is a free $\mathbf{Z}_p$-module of finite rank. We let $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ denote the set of irreducible representations of Δ over $\mathcal{F}$, always assuming that $\mathcal{F}$ is large enough so that irreducible $\mathcal{F}$-representations are absolutely irreducible. We extend the definition of $\lambda(X, \cdot)$ to arbitrary finite-dimension representations ρ of Δ by making the map $\lambda(X, \cdot)$ a homomorphism from the Grothendieck group $\mathcal{R}_{\mathcal{F}}(\Delta)$ to $\mathbf{Z}$.

Since $K \cap F_\infty = F$, we can identify Δ with $\mathrm{Gal}(K_\infty/F_\infty)$, where K_∞ is KF_∞, the cyclotomic $\mathbf{Z}_p$-extension of K. Hence there is a natural action of Δ on $\mathrm{Sel}_E(K_\infty)_p$. Assume that the Pontryagin dual of $\mathrm{Sel}_E(K_\infty)_p$ is a torsion Λ-module. If we take X to be that module, then we will denote $\lambda(X, \sigma)$ by $\lambda(E, \sigma)$. Let Σ_0 be a finite set of primes of F not lying above p or ∞. Then there is also a natural action of Δ on $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$. If we take X to be the Pontryagin dual of $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ (which will also be a torsion Λ-module), then we will denote $\lambda(X, \sigma)$ by $\lambda(E, \Sigma_0, \sigma)$. Although we will not discuss it here, one can also describe the difference $\lambda(E, \Sigma_0, \sigma) - \lambda(E, \sigma)$ in purely local terms. And so one can reduce the study of the $\lambda(E, \sigma)$'s to studying the $\lambda(E, \Sigma_0, \sigma)$'s for a suitable choice of Σ_0. Proposition 3.1 below concerns these non-primitive λ-invariants and is one of the main results of [12].

If v is a prime of F lying above p, we let $\overline{E}_v$ denote the reduction of E at v, an elliptic curve over the residue field of v. We let k_v denote the residue field for any prime of K lying above v.

Proposition 3.1. *Suppose that E has good ordinary reduction at the primes of F lying above p, that $E(K)[p] = 0$, that $\overline{E}_v(k_v)[p] = 0$ for all primes v of F lying over p, and that $\mathrm{Sel}_E(K_\infty)[p]$ is finite. Let Σ_0 be a finite set of primes containing $\Phi_{K/F}$, but not containing primes lying over p or ∞. Then the Pontryagin dual of $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ is a projective $\mathbf{Z}_p[\Delta]$-module.*

The assumption that $\mathrm{Sel}_E(K_\infty)[p]$ is finite implies that $\mathrm{Sel}_E(K_\infty)_p$ is Λ-cotorsion.

A corollary of the above result is that the invariants $\lambda(E, \Sigma_0, \rho)$ behave in the following way. Here we let ρ be an arbitrary representation of Δ over $\mathcal{F}$. Let $\mathcal{O}$ be the integers in $\mathcal{F}$. We can choose a Δ-invariant $\mathcal{O}$-lattice in the underlying representation space for ρ. Reducing modulo the maximal ideal $\mathfrak{m}$ of $\mathcal{O}$, we obtain a representation $\widetilde{\rho}$. Its semisimplification $\widetilde{\rho}^{ss}$ is well-defined. It is a representation over the residue field $\mathfrak{f} = \mathcal{O}/\mathfrak{m}$. Then, under the assumptions in the above proposition, we have the following result:

Corollary 3.2. *Suppose that the assumptions in proposition 3.1 are satisfied. Assume that ρ_1 and ρ_2 are representations of Δ such that $\widetilde{\rho}_1^{ss} \cong \widetilde{\rho}_2^{ss}$. Then $\lambda(E, \Sigma_0, \rho_1) = \lambda(E, \Sigma_0, \rho_2)$. That is, we have a linear relation*

$$\sum_\sigma m_1(\sigma)\lambda(E, \Sigma_0, \sigma) \;=\; \sum_\sigma m_2(\sigma)\lambda(E, \Sigma_0, \sigma)$$

where σ varies over the irreducible representations of Δ over $\mathcal{F}$ and $m_i(\sigma)$ denotes the multiplicity of σ in ρ_i for $i = 1, 2$.

If $\rho_1 \not\cong \rho_2$, but $\widetilde{\rho}_1^{ss} \cong \widetilde{\rho}_2^{ss}$, then the corresponding linear relation is nontrivial. Such nontrivial relations occur whenever $|\Delta|$ is divisible by p. We also remark that the conclusion in the corollary means that the map $\lambda(E, \Sigma_0, \cdot)$ from $\mathcal{R}_{\mathcal{F}}(\Delta)$ to $\mathbf{Z}$ factors through the reduction map $\mathcal{R}_{\mathcal{F}}(\Delta) \to \mathcal{R}_{\mathfrak{f}}(\Delta)$.

The assumptions in the corollary can be weakened. As shown in [12], one can omit the assumptions about $E(K)[p]$ and $\overline{E}_v(k_v)[p]$ for $v|p$. It suffices to assume that $\mathrm{Sel}_E(K_\infty)[p]$ is finite and that Σ_0 is chosen as in proposition 3.1. The Pontryagin dual of $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ may fail to be a projective $\mathbf{Z}_p[\Delta]$-module, but it still turns out to have a weaker property which we call *"quasi-projectivity"*. The linear relation in corollary 3.2 still follows. We call such a linear relation a *"congruence relation"* because it arises from an isomorphism $\widetilde{\rho}_1^{ss} \cong \widetilde{\rho}_2^{ss}$. We think of such an isomorphism as a congruence between the two representations ρ_1 and ρ_2. Note that the semisimplifications of $E[p] \otimes \widetilde{\rho}_1$ and $E[p] \otimes \widetilde{\rho}_2$ will also be isomorphic.

Assume now that Π is a normal subgroup of Δ and that Π is a p-group. Let $\Delta_0 = \Delta/\Pi$. Of course, $\Delta_0 = \mathrm{Gal}(K_0/F)$ for some subfield K_0 of K. Since $\mathfrak{f}$ has characteristic p, one sees easily that every irreducible representation of Δ over $\mathfrak{f}$ factors through Δ_0. A result in modular representation theory implies that if ρ_1 is a representation of Δ over $\mathcal{F}$, then there exists a representation ρ_2 of Δ which factors through Δ_0 such that $\widetilde{\rho}_1^{ss} \cong \widetilde{\rho}_2^{ss}$. Furthermore, one can show that $\mathrm{Sel}_E(K_\infty)[p]$ is finite if and only if $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite, where $K_{0,\infty}$ is the cyclotomic $\mathbf{Z}_p$-extension of K_0. Thus, it suffices to assume the finiteness of $\mathrm{Sel}_E(K_{0,\infty})[p]$. The corresponding congruence relation from corollary 3.2 then shows that $\lambda(E, \Sigma_0, \rho_1)$ can be expressed just in terms of the $\lambda(E, \Sigma_0, \sigma)$'s for $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta_0)$. Thus, the function $\lambda(E, \Sigma_0, \cdot)$ on $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ is completely determined by its restriction to $\mathrm{Irr}_{\mathcal{F}}(\Delta_0)$.

In the special case where Δ is itself a p-group, one obtains the simple formula $\lambda(E, \Sigma_0, \sigma) = \deg(\sigma)\lambda(E, \Sigma_0, \sigma_0)$, where σ_0 is the trivial representation of Δ. In this case, that formula was proven in [16]. It is stated there in a somewhat different form. One needs to assume that $\mathrm{Sel}_E(F_\infty)[p]$ is finite.

There are results of a similar nature in [3]. They concern irreducible Artin representations σ which factor through $\mathcal{G} = \mathrm{Gal}(\mathcal{K}/F)$, where $\mathcal{K}$ is generated over F by all the p-power roots of some $\alpha \in F^\times$ (subject to some mild restrictions on α). This is called a *"false Tate extension"* of F. Note that $\mathcal{G} = \mathrm{Gal}(\mathcal{K}/F)$ is a non-commutative p-adic Lie group of dimension 2. Since $\mathcal{K}$ contains μ_{p^∞}, the cyclotomic $\mathbf{Z}_p$-extension F_∞ of F is contained in $\mathcal{K}$. Therefore, the earlier assumption that $\mathcal{K} \cap F_\infty = F$ is not satisfied here. So we instead let $\Delta = \mathrm{Gal}(\mathcal{K}/F_\infty)$ and let $\Delta_0 = \mathrm{Gal}(F(\mu_{p^\infty})/F_\infty)$. Note that Δ_0 is cyclic and has order dividing $p-1$, and that the kernel Π of the map $\Delta \to \Delta_0$ is a pro-p group. These facts simplify the representation theory significantly, both in characteristic 0 and in characteristic p.

If σ' is an irreducible representation of Δ, one can define $\lambda(E, \sigma')$ essentially as before. One can then define $\lambda(E, \rho')$ for any representation ρ' of Δ. We define $\lambda(E, \sigma)$ to be $\lambda(E, \sigma|_\Delta)$ for all irreducible Artin representations σ of $\mathcal{G}$. The irreducible representations of Δ_0 are 1-dimensional. They are powers of ω, the p-power cyclotomic character which has order dividing $p-1$. Those characters are restrictions of characters of $\mathrm{Gal}(F(\mu_p)/F)$ to Δ. The results in section 4 of [3] give formulas for $\lambda(E, \sigma)$ in terms of the $\lambda(E, \omega^i)$'s under a certain hypothesis which we state below. Such formulas are also derived in [12], but under a somewhat different hypothesis.

We want to briefly discuss these hypotheses. Let $\mathcal{X}$ denote the Pontryagin dual of $\mathrm{Sel}_E(\mathcal{K})_p$. One can view $\mathcal{X}$ as a module over the completed group ring

$\mathbf{Z}_p[[\mathcal{G}]]$, the Iwasawa algebra for the 2-dimensional p-adic Lie group $\mathcal{G}$. The module $\mathcal{X}$ is finitely-generated over that ring. The key hypothesis in [3] is the following:

1: *$\mathcal{X}/\mathcal{X}_{tors}$ is finitely-generated as a $\mathbf{Z}_p[[\Delta]]$-module.*

Now it is known that $\mathbf{Z}_p[[\mathcal{G}]]$ is Noetherian. It follows that $\mathcal{X}_{tors}$ is killed by a fixed power of p. Note also that $\mathcal{X}/\mathcal{X}_{tors}$ is the Pontryagin dual of $\mathrm{Sel}_E(\mathcal{K})_{p,div}$. Under the above hypothesis, the results in [3] are proved by a K-theoretic approach. It may be possible to prove the results in [12] by such an approach. The proofs there work under the following hypothesis.

2: *$\mathrm{Sel}_{E'}\big(F(\mu_{p^\infty})\big)[p]$ is finite for at least one elliptic curve E' in the F-isogeny class of E.*

One can deduce hypothesis **1** from hypothesis **2**. However, the precise relationship between these hypotheses is not clear at present.

The results described in this section can be reformulated in another way. The analogy with the results mentioned in section 2 then becomes clearer. One can give an alternative definition of $\lambda(E,\sigma)$ as the $\mathcal{O}$-corank of a Selmer group over F_∞ associated to the $\mathcal{F}$-representation space $V_p(E)\otimes\sigma$ for G_{F_∞} One chooses a Galois invariant $\mathcal{O}$-lattice. We denote the corresponding quotient by $E[p^\infty]\otimes\sigma$, which is a discrete, divisible $\mathcal{O}$-module whose $\mathcal{O}$-rank is $2\mathrm{dim}_{\mathcal{F}}(\sigma)$. We then define a Selmer group essentially as for $E[p^\infty]$ itself. It is a subgroup of the Galois cohomology group $H^1(F_\infty, E[p^\infty]\otimes\sigma)$. For primes of F_∞ not lying over p, cocycle classes are required to be locally trivial. For primes π lying over p, cocycle classes are required to have a trivial image in $H^1(F_{\infty,\pi}, \overline{E}_\pi[p^\infty]\otimes\sigma)$.

The proof that $\lambda(E,\sigma)$ coincides with the $\mathcal{O}$-corank of $\mathrm{Sel}_{E[p^\infty]\otimes\sigma}(F_\infty)$ is a straightforward argument using the restriction maps for the global and local H^1's. Note that if ρ_1 and ρ_2 are representations of Δ and $\widetilde{\rho}_1^{ss}\cong\widetilde{\rho}_2^{ss}$, then

$$E[p]\otimes\widetilde{\rho}_1^{ss} \;\cong\; E[p]\otimes\widetilde{\rho}_2^{ss} \quad .$$

Thus, the residual representations for $V_p(E)\otimes\rho_1$ and $V_p(E)\otimes\rho_2$ will at least have isomorphic semisimplifications. Chapter 4 in [12] gives a proof of corollary 3.2 from this point of view, although only under more stringent hypotheses.

4. Parity

Continuing with the situation in section 3, the Birch and Swinnerton-Dyer conjecture for E over the field K asserts that the rank of $E(K)$ and the order of vanishing of the Hasse-Weil L-function $L(E,K,s)$ at $s=1$ should be the same. One can factor $L(E,K,s)$ as a product of L-functions $L(E,\sigma,s)$, where

σ varies over the irreducible representations of $\Delta = \mathrm{Gal}(K/F)$ over $\mathbf{C}$, each with multiplicity $\deg(\sigma)$. A refined form of the Birch and Swinnerton-Dyer conjecture asserts that, for every such σ, the multiplicity $r(E,\sigma)$ of σ in the $\mathbf{C}$-representation space $E(K) \otimes_{\mathbf{Z}} \mathbf{C}$ for Δ and the order of vanishing of $L(E,\sigma,s)$ at $s = 1$ should be the same. This refined conjecture is stated in [28] where it is derived from the Birch and Swinnerton-Dyer conjecture and a conjecture of Deligne and Gross.

The functional equation for $L(E,\sigma,s)$ relates that function to $L(E,\check{\sigma},2-s)$, where $\check{\sigma}$ is the contragredient of σ. If σ is self-dual (i.e., $\sigma \cong \check{\sigma}$), then that functional equation will have a root number $W(E,\sigma) \in \{\pm 1\}$ which would determine the parity of the order of vanishing at $s = 1$. The analytic continuation and functional equation for the L-functions mentioned above are conjectural in general, but there is a precise definition of $W(E,\sigma)$ due to Deligne [5]. General formulas for $W(E,\sigma)$ are derived in [30]. If one just considers the parity of the multiplicity and the order of vanishing, then one is led to conjecture that $W(E,\sigma) = (-1)^{r(E,\sigma)}$ for any self-dual representation σ of Δ.

It has proved easier to study a Selmer group version of the above conjecture. Fix embeddings of $\overline{\mathbf{Q}}$ into $\mathbf{C}$ and into $\overline{\mathbf{Q}}_p$. We can then realize σ as an irreducible representation of Δ over $\overline{\mathbf{Q}}$, and then over $\overline{\mathbf{Q}}_p$. Let $X_E(K)$ denote the Pontryagin dual of $\mathrm{Sel}_E(K)_p$. Let $s(E,\sigma)$ denote the multiplicity of σ in the $\overline{\mathbf{Q}}_p$-representation space $X_E(K) \otimes_{\mathbf{Z}_p} \overline{\mathbf{Q}}_p$. If the p-primary subgroup of the Tate-Shafarevich group for E over K is finite, then one has $s(E,\sigma) = r(E,\sigma)$. The parity conjecture that we will discuss here is the equality:

$$W(E,\sigma) \ = \ (-1)^{s(E,\sigma)} \tag{4}$$

for any self-dual irreducible representation of Δ. We will assume that p is odd.

There has been significant progress on this conjecture in certain cases. The first results go back to [1], and later [20], [15], and [24]. More recently, Nekovar ([25], [26]) proved the conjecture when E is defined over $\mathbf{Q}$ and has good ordinary reduction at p, and σ is trivial. This is now known for arbitrary elliptic curves over $\mathbf{Q}$. (See [7] and [19].) Subsequently, various results for more general self-dual Artin representations σ have been proved in [7], [8], which are part of a long series of papers, and in [22], [23]. Results in [3] and [12] also have a bearing on this question, as we will explain.

Under the assumption that $\mathrm{Sel}_E(K_\infty)_p$ is Λ-cotorsion, one can define $\lambda(E,\sigma)$ as before. Also, recall that self-dual irreducible representations σ of a finite group are of two types: orthogonal or symplectic. The following result is proved in [12].

Proposition 4.1. *Assume that σ is an irreducible orthogonal representation of Δ. Then we have $\lambda(E,\sigma) \equiv s(E,\sigma) \pmod 2$.*

One can use this result together with the congruence relations in section 3 to show that $W(E,\sigma)$ behaves well under congruences. To be precise, the following result is proven in [12]:

Proposition 4.2. *Assume that E has semistable reduction at the primes of F lying above* 2 *and* 3 *and that* $\mathrm{Sel}_E(K_\infty)[p]$ *is finite. Let σ_1 and σ_2 be irreducible orthogonal representations of Δ. Assume that $\widetilde{\sigma}_1^{ss} \cong \widetilde{\sigma}_2^{ss}$. Then* (4) *holds for $\sigma = \sigma_1$ if and only if* (4) *holds for $\sigma = \sigma_2$.*

There is also a version for arbitrary orthogonal representations ρ of Δ. This kind of result is proven in [12] with a significantly weaker assumption concerning the primes above 2 or 3. It should be possible to eliminate that assumption entirely. As for symplectic irreducible representations σ, one has $W(E, \sigma) = 1$, and so one expects $s(E, \sigma)$ to be even. There seem to be no results known in that direction. However, it is not hard to show that $r(E, \sigma)$ is even if σ is symplectic. Thus, if the p-primary subgroup of the Tate-Shafarevich group for E over K is finite, then $s(E, \sigma)$ is indeed even.

In the rest of this article, we will consider the situation mentioned in section 3 where $\Delta = \mathrm{Gal}(K/F)$ has a normal p-subgroup Π, K_0 is the fixed field for Π, and $\Delta_0 = \mathrm{Gal}(K_0/F)$. We assume that $K \cap F_\infty = F$ and let $K_{0,\infty}$ be K_0F_∞, the cyclotomic $\mathbf{Z}_p$-extension of K_0. One can show that $\mathrm{Sel}_E(K_\infty)[p]$ is finite if and only if $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite. Let us assumes the finiteness of $\mathrm{Sel}_E(K_{0,\infty})[p]$ and the semistability assumption for primes above 2 and 3 in proposition 4.2. One can then derive the following consequence: *If* (4) *is valid for all irreducible orthogonal representations factoring through Δ_0, then* (4) *is valid for all irreducible orthogonal representations factoring through Δ.*

As an illustration, one can consider subfields of $F(A[p^\infty])$, where A is an elliptic curve defined over F. We will assume that the homomorphism $\mathrm{G}_F \to \mathrm{Aut}_{\mathbf{Z}_p}\big(T_p(A)\big)$ giving the action of G_F on $T_p(A)$ is surjective. Thus, $\mathrm{Gal}\big(F(A[p^\infty])/F\big) \cong \mathrm{GL}_2(\mathbf{Z}_p)$ and so $F(A[p^\infty])$ will contain a tower of subfields K_n such that $\Delta_n = \mathrm{Gal}(K_n/F)$ is isomorphic to $\mathrm{PGL}_2(\mathbf{Z}/p^{n+1}\mathbf{Z})$ for all $n \geq 0$. Let $\mathcal{K} = \cup_n K_n$. We will consider Artin representations over F which factor through $\mathrm{Gal}(\mathcal{K}/F)$, and hence through Δ_n for some $n \geq 0$.

To apply the results in [12] to $K = K_n$ for any $n \geq 0$, one may just assume that $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite. It turns out that all irreducible representations of $\mathrm{PGL}_2(\mathbf{Z}/p^{n+1}\mathbf{Z})$ are self-dual and orthogonal. Thus, under the assumptions about E in proposition 4.2 (or various alternative hypotheses), it follows that (4) holds for all the irreducible Artin representations factoring through $\mathrm{Gal}(\mathcal{K}/\mathbf{Q})$ if it holds for all irreducible Artin representations factoring through $\Delta_0 = \mathrm{Gal}(K_0/F)$. Two of those Artin representations factoring through Δ_0 are 1-dimensional, two are p-dimensional, and all the other irreducible Artin representations of $\mathrm{Gal}(\mathcal{K}/\mathbf{Q})$ are even dimensional. If one just assumes that (4) is valid for the four odd-dimensional irreducible representations σ just mentioned, then one finds that (4) is valid for a certain infinite family of irreducible Artin representations σ.

Assume that $F = \mathbf{Q}$, that $A = E$, and that the surjectivity hypothesis in the previous paragraph is satisfied. Then (4) is valid for the two 1-dimensional representations of Δ_0. This follows from the results of Nekovar, Kim, and of T. and V. Dokchitser cited above. Under mild hypotheses on the reduction type, one then obtains (4) for the two p-dimensional Artin representations factoring through Δ_0. This follows from a result proven in [3], and also in [6] under certain stronger hypotheses, establishing (4) when σ is trivial and E is an elliptic curve without complex multiplication which has an isogeny of degree p over the base field. One applies this result to certain subfields of K_0.

The results in [3] about the parity conjecture (4) have a similar form. They concern irreducible orthogonal Artin representations which factor through the Galois group $\mathcal{G} = \mathrm{Gal}(\mathcal{K}/F)$, where $\mathcal{K}$ is a p-adic Lie extension of F. A key assumption in [3] is hypothesis **1** discussed in section 3. One takes $\Delta = \mathrm{Gal}(\mathcal{K}/F_\infty)$. The cases considered in that paper have the following property: Δ has a normal pro-p subgroup Π such that $\Delta_0 = \Delta/\Pi$ is abelian and of order prime to p. One can identify Δ_0 with a quotient of $\mathcal{G}$. In addition to the case where $\mathcal{K}$ is the false Tate extension mentioned in section 3, they consider the case where $\mathcal{K} = F(E[p^\infty])$, E is an elliptic curve without complex multiplication, and E has an isogeny of degree p over F. The result cited in the previous paragraph concerning such an elliptic curve establishes (4) for the self-dual irreducible representations of Δ_0, i.e., the characters of Δ_0 of order 1 or 2. Under some mild additional hypotheses, they can then prove (4) for all the other irreducible orthogonal Artin representations which factor through $\mathcal{G}$.

Mazur and Rubin [22] study the case where $\Delta = \mathrm{Gal}(K/F)$ is a dihedral group of order $2p^n$ for $n \geq 1$. One can then take Δ_0 to be the quotient group of Δ of order 2. Let K_0 be the corresponding quadratic extension of F. All the irreducible representations of Δ are orthogonal. There are two of degree 1, which we call ε_0 and ε_1. They factor through Δ_0. If σ is an irreducible representation of Δ which does not factor through Δ_0, then σ has degree 2. Furthermore, we have $\widetilde{\sigma}^{ss} \cong \widetilde{\varepsilon}_0 \oplus \widetilde{\varepsilon}_1$. Note also that the $\mathbf{Z}_p$-corank of $\mathrm{Sel}_E(K_0)_p$ is equal to $s(E, \varepsilon_0) + s(E, \varepsilon_1)$. The results in [22] are stated under an assumption about the parity of the $\mathbf{Z}_p$-corank of $\mathrm{Sel}_E(K_0)_p$. In essence, and under various rather mild sets of hypotheses, the results in [22] establish (4) for the σ's of degree 2 under the assumption that

$$W(E, \varepsilon_0)W(E, \varepsilon_1) \;=\; (-1)^{s(E,\varepsilon_0)+s(E,\varepsilon_1)} \quad .$$

This assumption is somewhat weaker than the assumption that (4) is valid for the irreducible representations factoring through Δ_0, namely ε_0 and ε_1. Mazur and Rubin use such a result to show that the $\mathbf{Z}_p$-corank of $\mathrm{Sel}_E(K)_p$ is large for certain Galois extensions K/F. Such an assertion follows under hypotheses which imply that $W(E, \sigma) = -1$ for many self-dual irreducible representations σ of $\mathrm{Gal}(K/F)$. If $s(E, \sigma)$ is odd, then $s(E, \sigma)$ is positive. This idea is exploited in [23]. It is also pursued in [3] and [12], although much more conditionally.

One can define $W(E, \rho)$ for any self-dual Artin representation ρ over a number field F. One can also extend the definition of $s(E, \cdot)$ to all Artin representations ρ over F. Then (4) can be restated as

$$W(E, \rho) \;=\; (-1)^{s(E,\rho)} \tag{5}$$

for all self-dual Artin representations ρ over F. Following the theme of this article, one would like to prove that the validity of (5) is preserved by congruences. That is, if (5) is valid for ρ_1 and if $\widetilde{\rho}_1^{ss} \cong \widetilde{\rho}_2^{ss}$, then (5) should also be valid for ρ_2. We believe that such a result is approachable. The results in [22] discussed above go a long way in the case where Δ is a dihedral group of order $2p^n$. There are also remarkable results concerning (5) in [7] which go a long way in the case where Δ_0 is abelian and also in the case where ρ is a permutation representation.

References

[1] B. J. Birch, N. Stephens, *The parity of the rank of the Mordell-Weil group*, Topology **5** (1966), 295–299.

[2] S. Bloch, K. Kato, *L-functions and Tamagawa numbers of motives*, in the Grothendieck Festschrift, Progress in Math. I, **86**, Birkhäuser (1990), 333–400.

[3] J. Coates, T. Fukaya, K. Kato, R. Sujatha, *Root numbers, Selmer groups, and non-commutative Iwasawa theory*, J. Algebraic Geom. **19** (2010), 19–97.

[4] J. Coates, R. Greenberg, *Kummer theory for abelian varieties over local fields*, Invent. Math. **124** (1996), 129–174.

[5] P. Deligne, *Les constantes des équations fonctionelles des fonctions L*, in Modular Functions of One Variable II, Lect. Notes in Math. **349** (1973), 501–595.

[6] T. Dokchitser, V. Dokchitser, *Parity of ranks for elliptic curves with a cyclic isogeny*, J. Number Theory **128** (2008), 662–679.

[7] T. Dokchitser, V. Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math. **178** (2009), 23–71.

[8] T. Dokchitser, V. Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, to appear in Annals of Math.

[9] M. Emerton, R. Pollack, T. Weston, *Variation of Iwasawa invariants in Hida families*, Invent. Math. **163** (2006), 523–580.

[10] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. **73** (1983), 349–366.

[11] R. Greenberg, *Iwasawa theory for p-adic representations*, Advanced Studies in Pure Math. **17** (1989), 97–137.

[12] R. Greenberg, *Iwasawa theory, projective modules, and modular representations*, to appear in Memoirs of the Amer. Math. Soc.

[13] R. Greenberg, A. Iovita, R. Pollack, *On the Iwasawa invariants of elliptic curves with supersingular reduction*, in preparation.

[14] R. Greenberg, V. Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), 17–63.

[15] L. Guo, *General Selmer groups and critical values of Hecke L-functions*, Math. Ann. **297** (1993), 221–233.

[16] Y. Hachimori, K. Matsuno, *An analogue of Kida's formula for the Selmer groups of elliptic curves*, J. Alg. Geom. **8** (1999), 581–601.

[17] H. Hida, *Galois representations into* $\mathbf{Z}_p[[X]]$ *attached to ordinary cusp forms*, Invent. Math. **85** (1986), 545–613.

[18] K. Kato, *p-adic Hodge theory and values of zeta functions of modular curves*, Astérisque **295** (2004), 117–290.

[19] B. D. Kim, *The parity conjecture for elliptic curves at supersingular reduction primes*, Comp. Math. **143** (2007), 47–72.

[20] K. Kramer and J. Tunnell, *Elliptic curves and local* ϵ*-factors*, Comp. Math. **46** (1982), 307–352.

[21] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

[22] B. Mazur, K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. **166** (2007), 579–612.

[23] B. Mazur, K. Rubin, *Growth of Selmer rank in nonabelian extensions of number fields*, Duke Math. Jour. **143** (2008) 437–461.

[24] P. Monsky, *Generalizing the Birch-Stephens theorem*, Math. Zeit. **221** (1996), 415–420.

[25] J. Nekovář, *On the parity of ranks of Selmer groups II*, Comptes Rendus de l'Acad. Sci. Paris, Serie I, **332** (2001), No. 2, 99–104

[26] J. Nekovář, Selmer complexes, Astérisque **310** (2006).

[27] R. Pollack, T. Weston, *Mazur-Tate elements of non-ordinary modular forms*, preprint.

[28] D. Rohrlich, *The vanishing of certain Rankin-Selberg convolutions*, in Automorphic Forms and Analytic Number Theory, Les publications CRM, Montreal, 1990, 123–133.

[29] D. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. **75** (1984), 404–423.

[30] D. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Comp. Math. **100** (1996), 311–349.

[31] K. Rubin, *On the main conjecture of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **93** (1988), 701–713.

[32] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), 25–68.

[33] K. Rubin and A. Silverberg, *Families of elliptic curves with constant mod p representations*, Elliptic curves, modular forms, and Fermat's last theorem, Hong Kong, International Press, 1993.

[34] P. Schneider, *p-Adic height pairings II*, Invent. Math. **79** (1985), 329–374.