Selmer groups and congruences

Ralph Greenberg

Department of Mathematics
University of Washington
Seattle, Washington, USA

International Congress of Mathematicians
August 19th-27th, 2010
Hyderabad, India

The Mordell-Weil Theorem

Suppose that E is an elliptic curve defined over a number field F. Let $E(F)$ denote the set of points on E with coordinates in the field F. Under a certain simply defined group operation, $E(F)$ becomes an abelian group, the Mordell-Weil group for E over F.

We recall the classical Mordell-Weil Theorem.

Mordell-Weil Theorem. *Suppose that E is an elliptic curve defined over a number field F. Then $E(F)$ is a finitely generated abelian group. That is,*

$$E(F) \cong \mathbf{Z}^r \times T \quad ,$$

where $r = \mathrm{rank}\big(E(F)\big)$ is a nonnegative integer and T is a finite abelian group.

Two examples

Two specific examples will occur later in this talk. We take $F = \mathbf{Q}$.

$E_1 \ : \ y^2 = x^3 + x - 10.$

We have $E_1(\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z}$. It is generated by $(2, 0)$. Thus, $\mathrm{rank}\big(E_1(\mathbf{Q})\big) = 0$.

$E_2 \ : \ y^2 = x^3 - 584x + 5444.$

We have $E_2(\mathbf{Q}) \cong \mathbf{Z}$. It is generated by $(-8, 98)$. Thus, $\mathrm{rank}\big(E_2(\mathbf{Q})\big) = 1$.

Selmer groups

A crucial ingredient in the proof of the Mordell-Weil theorem is to show that $E(F)/nE(F)$ is finite for at least one $n \geq 2$. Actually, one shows that $E(F)/nE(F)$ is finite for all n by defining a map from $E(F)/nE(F)$ to the Selmer group for E over K and showing that the kernel and the image of that map are both finite.

We will regard F as a subfield of $\overline{\mathbf{Q}}$, a fixed algebraic closure of $\mathbf{Q}$. Let E_{tors} denote the torsion subgroup of $E(\overline{\mathbf{Q}})$. Then

$$E_{tors} \cong (\mathbf{Q}/\mathbf{Z})^2$$

as a group. One has a natural action of $\mathrm{G}_F = \mathrm{Gal}(\overline{\mathbf{Q}}/F)$ on E_{tors}.

The Selmer group for E over F will be denoted by $\mathrm{Sel}_E(F)$. It 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.

Kummer theory for E

We will write $H^1(F, E_{tors})$ instead of $H^1(G_F, E_{tors})$. If $P \in E(F)$ and $n \geq 1$, then there exists a point $Q \in E(\overline{\mathbf{Q}})$ such that

$$nQ = P \quad .$$

If $g \in \mathrm{G}_F = \mathrm{Gal}(\overline{\mathbf{Q}}/F)$, then $Q' = g(Q)$ also satisfies $nQ' = P$. Thus, $g(Q) - Q = Q' - Q \in E_{tors}$. The map

$$\varphi : G_F \to E_{tors} \qquad \text{defined by } \varphi(g) = g(Q) - Q$$

is a 1-cocycle and defines a class $[\varphi]$ in $H^1(F, E_{tors})$. In this way, we can define the *"Kummer map"*

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

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

The definition of the Selmer group.

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

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

where F_v is the completion of F at v. One can identify G_{F_v} with a subgroup of G_F and thereby define a restriction map

$$H^1(F, E_{tors}) \; \longrightarrow \; H^1(F_v, E_{tors}) \quad .$$

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

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

where v runs over all the primes of F. One shows that the image of σ is actually contained in the direct sum.

Properties of the Selmer group

Note that $E(F) \otimes_{\mathbf{Z}} (\mathbf{Q}/\mathbf{Z}) \cong (\mathbf{Q}/\mathbf{Z})^r$, where $r = \operatorname{rank}\big(E(F)\big)$. The image of the Kummer map κ is clearly a subgroup of $\mathrm{Sel}_E(F)$.

Thus, $\mathrm{Sel}_E(F)$ contains a subgroup isomorphic to $\big(\mathbf{Q}/\mathbf{Z}\big)^r$, namely $\mathrm{im}(\kappa)$. The corresponding quotient group $\mathrm{Sel}_E(F)\big/\mathrm{im}(\kappa)$ is called the Tate-Shafarevich group for E over F.

It is conjectured that the Tate-Shafarevich group is finite. If this is so, then $\mathrm{im}(\kappa)$ is precisely the maximal divisible subgroup of $\mathrm{Sel}_E(F)$, and one can then recover the value of r from the structure of the $\mathrm{Sel}_E(F)$.

The weak Mordell-Weil theorem

Note that $E(F)/nE(F) \cong E(F) \otimes \left(\frac{1}{n}\mathbf{Z}/\mathbf{Z}\right)$. The proof that this group is finite proceeds by showing that the composite map

$$E(F) \otimes \left(\tfrac{1}{n}\mathbf{Z}/\mathbf{Z}\right) \longrightarrow E(F) \otimes \left(\mathbf{Q}/\mathbf{Z}\right) \longrightarrow \mathrm{Sel}_E(F)$$

has finite kernel and image. The first map has finite kernel and the second map is injective. Hence the kernel of the composite map is finite. The image of that map is contained in $\mathrm{Sel}_E(F)[n]$, and this is known to be a finite group for all n.

The p-primary subgroup of $\mathrm{Sel}_E(F)$

The Selmer group $\mathrm{Sel}_E(F)$ is a torsion group. For every prime p, its p-primary subgroup will be denoted by $\mathrm{Sel}_E(F)_p$. It is known that

$$\mathrm{Sel}_E(F)_p \;\cong\; (\mathbf{Q}_p/\mathbf{Z}_p)^{s_p} \times A_p \quad ,$$

where s_p is a nonnegative integer and A_p is a finite abelian p-group.

The integer s_p is called the $\mathbf{Z}_p$-corank of $\mathrm{Sel}_E(F)_p$. If the Tate-Shafarevich group for E over F is finite, as is conjectured to be so, then $s_p = r$ for all primes p, where $r = \mathrm{rank}\big(E(F)\big)$.

Note that $\mathbf{Q}_p/\mathbf{Z}_p$ is isomorphic to $(\mathbf{Q}/\mathbf{Z})_p$, the p-primary subgroup of $\mathbf{Q}/\mathbf{Z}$. Note also that $\big(\mathbf{Q}_p/\mathbf{Z}_p\big)[p]$ has $\mathbf{F}_p$-dimension 1.

A theorem of Faltings

The Galois group G_F acts on E_{tors}. A theorem of Faltings implies that the elliptic curve is determined up to isogeny over F by the action of G_F on E_{tors}. Let p be a prime and let $n \geq 0$. The p^n-torsion on E will be denoted by $E[p^n]$. We will let $E[p^\infty]$ denote the union of the $E[p^n]$'s. The inverse limit of the $E[p^n]$'s is the p-adic Tate module $T_p(E)$. Let $V_p(E) = T_p(E) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, a two-dimensional vector space over $\mathbf{Q}_p$. All of these objects have a continuous action of G_F.

It was conjectured by Tate and proved by Faltings that E is determined up to isogeny over F by the action of G_F on $V_p(E)$. The action of G_F on $T_p(E)$, or equivalently on $E[p^\infty]$, determines E up to an isogeny defined over F whose kernel has order (which is the so-called "degree of the isogeny") prime to p.

A valuable insight

Suppose that E and E' are elliptic curves defined over F and that there is an isogeny from E to E' over F of degree prime to p. Then one can show that $\mathrm{Sel}_E(F)_p$ and $\mathrm{Sel}_{E'}(F)_p$ are isomorphic. Thus, the above theorem of Faltings raises the question of whether one can somehow define $\mathrm{Sel}_E(F)_p$ just in terms of the Galois module $E[p^\infty]$. This turns out to be so.

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 by myself 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 for the purpose of generalizing the Birch and Swinnerton-Dyer conjecture.

Defining $\mathrm{Sel}_E(F)_p$.

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 $\mathrm{Sel}_E(F)_p$.

We next discuss briefly how this can be done.

The map $\kappa_{v,p}$

The p-primary subgroup of $E(F_v) \otimes_{\mathbf{Z}} (\mathbf{Q}/\mathbf{Z})$ is $E(F_v) \otimes_{\mathbf{Z}} (\mathbf{Q}_p/\mathbf{Z}_p)$. The map $\kappa_{v,p}$ is an injective homomorphism

$$\kappa_{v,p} : \; E(F_v) \otimes_{\mathbf{Z}} (\mathbf{Q}_p/\mathbf{Z}_p) \; \longrightarrow \; H^1(F_v, E[p^\infty]) \quad .$$

The structure of $E(F_v) \otimes_{\mathbf{Z}} (\mathbf{Q}_p/\mathbf{Z}_p)$ depends on whether v divides p or not.

The image of $\kappa_{v,p}$ when $v \nmid p$.

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.

The image of $\kappa_{v,p}$ when $v|p$.

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 $\mathbf{F}_v$. Considering the p-power torsion, one has an exact sequence

$$0 \longrightarrow C_v \longrightarrow E[p^\infty] \longrightarrow \overline{E}_v[p^\infty] \longrightarrow 0 \quad .$$

The reduction is ordinary if the integer

$$a_v \;=\; a_v(E) \;=\; 1 + |\mathbf{F}_v| - |\overline{E}_v(\mathbf{F}_v)|$$

is not divisible by p. Equivalently, ordinary reduction at v means $\overline{E}_v[p^\infty]$ is isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$ as a group. It then turns out that C_v is also isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$.

$im(\kappa_{v,p})$ when $v|p$, continued

Remarkably, one has the following description of the image of $\kappa_{v,p}$:

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

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.

A general description of $\mathrm{im}(\kappa_{v,p})$

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. 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 map

$$H^1\big(F_v, V_p(E)\big) \longrightarrow H^1\big(F_v, V_p(E) \otimes_{\mathbf{Q}_p} B_{crys}\big) \quad .$$

One has $V_p(E)/T_p(E) \cong E[p^\infty]$. Then, it turns out that $\mathrm{im}(\kappa_{v,p})$ is precisely 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 finite Galois module $E[p]$

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.

The elliptic curves E_1 and E_2 mentioned previously illustrate this point. Take $F = \mathbf{Q}$. In fact, it turns out that

$$\mathrm{Sel}_{E_1}(\mathbf{Q}) = 0 \quad , \qquad \mathrm{Sel}_{E_2}(\mathbf{Q}) \cong \mathbf{Q}/\mathbf{Z}$$

Take $p = 5$. It can be shown that $E_1[5] \cong E_2[5]$ as $G_{\mathbf{Q}}$-modules. But $\mathrm{Sel}_{E_1}(\mathbf{Q})[5]$ and $\mathrm{Sel}_{E_2}(\mathbf{Q})[5]$ obviously have different $\mathbf{F}_5$-dimensions.

Congruences

$E_1[p] \cong E_2[p]$ means that $T_p(E_1)/pT_p(E_1) \cong T_p(E_2)/pT_p(E_2)$.

We can think of such an isomorphism as a congruence modulo p between the p-adic Tate modules $T_p(E_1)$ and $T_p(E_2)$.

It can also be interpreted in terms of the integers a_v mentioned earlier. It means that

$$a_v(E_1) \equiv a_v(E_2) \pmod{p}$$

for all but finitely many primes v of F.

In the next part of this talk, 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.

The cyclotomic $\mathbf{Z}_p$-extension of F

We fix a prime p. Let μ_{p^∞} denote the group of p-power roots of unity in $\overline{\mathbf{Q}}$. The cyclotomic $\mathbf{Z}_p$-extension of F is a subfield F_∞ of $F(\mu_{p^\infty})$, the field generated over F by μ_{p^∞}. The field F_∞ is characterized by the fact that $\Gamma = \mathrm{Gal}(F_\infty/F)$ is isomorphic to the additive group $\mathbf{Z}_p$. Thus, $F_\infty = \cup_{n\geq 0}\, F_n$, where F_n is a cyclic extension of F of degree p^n.

We will usually take $F = \mathbf{Q}$, partly for simplicity, but also because some of the results that we state depend on deep theorems of Kato and Rohrlich which are valid if $F/\mathbf{Q}$ is abelian, and in particular when $F = \mathbf{Q}$. The cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$ is $\mathbf{Q}_\infty$.

We will assume from here on that p is odd and that the elliptic curves have good ordinary reduction at p.

The p-Selmer group over $\mathbf{Q}_\infty$

Everything that we said before about describing $\mathrm{Sel}_E(F)_p$ can be easily extended to arbitrary subfields F of $\overline{\mathbf{Q}}$. In particular, we will concentrate on $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$. Assume that E is defined over $\mathbf{Q}$. The theorem of Kato and Rohrlich mentioned above implies that the $\mathbf{Z}_p$-corank of $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$ is finite. This was conjectured to be so by Mazur in the early 1970s and means that

$$\mathrm{Sel}_E(\mathbf{Q}_\infty)_p \;\cong\; \left(\mathbf{Q}_p/\mathbf{Z}_p\right)^{\lambda(E)} \times A_p \quad ,$$

where $\lambda(E)$ is a nonnegative integer (which depends on p) and A_p has finite exponent. Sometimes A_p is infinite. If E has no isogenies over $\mathbf{Q}$ of degree p, then it is conjectured that A_p is finite. If that is the case, then one can show that $A_p = 0$, i.e., that

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

Properties of $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$

We will often assume that $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p[p]$ is finite. Then

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

Note that if this is the case, then $\lambda(E) = \dim_{\mathbf{F}_p}\left(\mathrm{Sel}_E(\mathbf{Q}_\infty)_p[p]\right)$.

The definition of $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$ can be put in the following form:

$$\mathrm{Sel}_E(\mathbf{Q}_\infty)_p \;=\; \ker\left(H^1(\mathbf{Q}_\infty, E[p^\infty]) \longrightarrow \bigoplus_\ell \mathcal{H}_\ell(\mathbf{Q}_\infty, E[p^\infty])\right) \quad ,$$

where ℓ varies over all primes and $\mathcal{H}_\ell(\mathbf{Q}_\infty, E[p^\infty])$ denotes the direct sum of the $H^1(\mathbf{Q}_{\infty,\eta}, E[p^\infty])/\mathrm{im}(\kappa_{\eta,p})$'s over all primes η of $\mathbf{Q}_\infty$ lying over a prime ℓ.

The non-primitive Selmer groups

If $\ell \neq p$, the local cohomology groups $H^1(\mathbf{Q}_{\infty,\eta}, E[p^\infty])$ for $\eta|\ell$ are relatively easy to study. One finds that

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

where $\delta(E,\ell)$ is a nonnegative integer which is easily determined.

Let Σ_0 be a finite set of primes. Assume that $p \notin \Sigma_0$. We define a *"non-primitive"* Selmer group by

$$\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)_p \;=\; \ker\left(H^1(\mathbf{Q}_\infty, E[p^\infty]) \longrightarrow \bigoplus_{\ell \notin \Sigma_0} \mathcal{H}_\ell(\mathbf{Q}_\infty, E[p^\infty])\right) \;.$$

Thus, we are omitting the local triviality conditions for the finite set of primes in Σ_0. Obviously, we have

$$\mathrm{Sel}_E(\mathbf{Q}_\infty)_p \;\subseteq\; \mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)_p \;.$$

Properties of $\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)_p$

The map whose kernel is $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$ turns out to be surjective. It follows that

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

From the previously slide, we have

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

where $\delta(E,\Sigma_0) = \sum_{\ell\in\Sigma_0} \delta(E,\ell)$.

Properties of $\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)_p$

Under the assumption that $\mathrm{Sel}_E(\mathbf{Q}_\infty)[p]$ is finite, $\mathrm{Sel}_E(\mathbf{Q}_\infty)_p$ is divisible, and so we will then have

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

Consequently, we have

$$\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)_p \;\cong\; \left(\mathbf{Q}_p/\mathbf{Z}_p\right)^{\lambda(E,\Sigma_0)} \quad ,$$

where $\lambda(E, \Sigma_0) = \lambda(E) + \delta(E, \Sigma_0)$.

Note that $\lambda(E, \Sigma_0) = \dim_{\mathbf{F}_p}\left(\mathrm{Sel}_E^{\Sigma_0}(\mathbf{Q}_\infty)[p]\right)$, assuming as before that $\mathrm{Sel}_E(\mathbf{Q}_\infty)[p]$ is finite.

Comparing the λ-invariants when $E_1[p] \cong E_2[p]$.

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. As mentioned before, 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 has bad reduction. Under these assumptions, one can prove that

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

Consequently, if $\mathrm{Sel}_{E_1}^{\Sigma_0}(\mathbf{Q}_\infty)[p]$ is finite, then so is $\mathrm{Sel}_{E_2}^{\Sigma_0}(\mathbf{Q}_\infty)[p]$.

Comparing the λ-invariants when $E_1[p] \cong E_2[p]$, continued

Continuing to assume that $E_1[p] \cong E_2[p]$ and that Σ_0 is chosen as above, the $\mathbf{F}_p$-dimensions of $\mathrm{Sel}_{E_1}^{\Sigma_0}(\mathbf{Q}_\infty)[p]$ and $\mathrm{Sel}_{E_2}^{\Sigma_0}(\mathbf{Q}_\infty)[p]$ will be the same. That is, we have

$$\lambda(E_1, \Sigma_0) \;=\; \lambda(E_2, \Sigma_0)$$

and so one 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 $\lambda(E_1)$.

In summary,

In summary, we have the following theorem:

Theorem A. *Suppose that E_1 and E_2 are elliptic curves defined over $\mathbf{Q}$ with good, ordinary reduction at p. Assume that p is an odd prime, that $E_1[p] \cong E_2[p]$ for the action of $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, and that $E_1[p]$ is irreducible. Assume that $\mathrm{Sel}_{E_1}(\mathbf{Q}_\infty)[p]$ is finite. Let Σ_0 be a finite set of primes containing all primes where E_1 or E_2 has bad reduction, but not containing p. Then we have*

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

Therefore, we have $\lambda(E_1) + \delta(E_1, \Sigma_0) \;=\; \lambda(E_2) + \delta(E_2, \Sigma_0)$.

An example

As an example, consider the two elliptic curves

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

mentioned previously. They have conductors $52 = 4 \cdot 13$ and $364 = 4 \cdot 7 \cdot 13$, 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 $\mathrm{Sel}_{E_1}(\mathbf{Q}_\infty)_5 = 0$. 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 $\lambda(E_2) = 5$. That is, we have

$$\mathrm{Sel}_{E_2}(\mathbf{Q}_\infty)_5 \;\cong\; (\mathbf{Q}_5/\mathbf{Z}_5)^5 \quad .$$

Abundance of examples of congruences

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 by Rubin and Silverberg 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 Hecke eigenforms 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 the Hecke eigenforms under consideration. 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.

The results described above are from a paper by myself and Vinayak Vatsal. Our purpose was to show that a certain conjecture, the so-called Main Conjecture of Iwasawa Theory for elliptic curves (and more generally for Hecke eigenforms), is preserved by congruences. Under the assumptions that we have been making, if the main conjecture is valid for E_1, then it is also valid for E_2.

For the specific example considered on the previous slide, where $p = 5$, the main conjecture is quite easy to verify for E_1, and therefore will also be true for E_2.

Another approach

A somewhat different approach is taken by Emerton, Pollack, and Weston. Their 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.

If f is such an eigenform, then there is a natural Galois module A_f (which is the analogue for f of $E[p^\infty]$). One can define a natural Selmer group for A_f over $\mathbf{Q}_\infty$.

Another approach

The above authors define a certain Selmer group for a Galois module $A_f[\pi]$ (the analogue of $E[p]$) in such a way that one has an isomorphism

$$\mathrm{Sel}_{A_f[\pi]}(\mathbf{Q}_\infty) \;\cong\; \mathrm{Sel}_{A_f}(\mathbf{Q}_\infty)[\pi] \quad .$$

However, the local conditions defining the Selmer group for $A_f[\pi]$ depend on both the Galois module $A_f[\pi]$ and some data involving f itself. If f_1 and f_2 are two such eigenforms, one can then determine the difference between the coranks of the Selmer groups for A_{f_1} and A_{f_2} by examining the difference in those local conditions.

Artin twists

Suppose that E is defined over $\mathbf{Q}$ and p is a prime where E has good ordinary reduction. The talk so far has concerned 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. Suppose that K is a finite Galois extension of $\mathbf{Q}$ and that $K \cap \mathbf{Q}_\infty = \mathbf{Q}$. The Artin representations to be considered will factor through

$$\Delta \;=\; \mathrm{Gal}(K/\mathbf{Q}) \quad .$$

That is, σ will be a finite-dimensional representation of the Galois group Δ.

Artin twists

However, if K is allowed to vary over the finite extensions of $\mathbf{Q}$ contained in some infinite Galois extension $\mathcal{K}$ of $\mathbf{Q}$ satisfying $\mathcal{K} \cap \mathbf{Q}_\infty = \mathbf{Q}$, then σ can vary over all Artin representations over $\mathbf{Q}$ which factor through $\mathrm{Gal}(\mathcal{K}/\mathbf{Q})$.

One interesting case is where $\mathrm{Gal}(\mathcal{K}/\mathbf{Q})$ is a p-adic Lie group. One can then often describe interesting infinite families of irreducible Artin representations σ that factor through $\mathrm{Gal}(\mathcal{K}/\mathbf{Q})$.

Some notation

If ℓ is a prime, let $e(K, \ell)$ denote the ramification index for ℓ in the extension $K/\mathbf{Q}$. Let

$$\Phi_K \;=\; \{\ell \mid \ell \neq p \text{ and } e(K,\ell) \text{ is divisible by } p\ \} \quad .$$

This finite set of primes will play an important role in this part of the talk.

Let $K_\infty = K\mathbf{Q}_\infty$. Then K_∞ is the cyclotomic $\mathbf{Z}_p$-extension of K. Since $K \cap \mathbf{Q}_\infty = \mathbf{Q}$, we have

$$\mathrm{Gal}(K_\infty/\mathbf{Q}) \;\cong\; \Delta \times \Gamma$$

and both $\Delta = \mathrm{Gal}(K_\infty/\mathbf{Q}_\infty)$ and $\Gamma = \mathrm{Gal}(K_\infty/\mathbf{Q}_\infty)$ act on $\mathrm{Sel}_E(K_\infty)_p$.

A representation space for Δ

We will assume that $\mathrm{Sel}_E(K_\infty)_p[p]$ is finite. Then $\mathrm{Sel}_E(K_\infty)_p$ has finite $\mathbf{Z}_p$-corank and we can form a finite dimension representation space for Δ over $\mathbf{Q}_p$ as follows: Let $X_E(K_\infty)$ denote the Pontryagin dual of $\mathrm{Sel}_E(K_\infty)_p$, which is a $\mathbf{Z}_p$-module of finite rank. Let

$$V_E(K_\infty) = X_E(K_\infty) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \quad .$$

Its dimension will be denoted by $\lambda(E, K)$ and is equal to the $\mathbf{Z}_p$-corank of $\mathrm{Sel}_E(K_\infty)_p$.

Suppose that Σ_0 is a finite set of primes of $\mathbf{Q}$ as before. We assume that $p \notin \Sigma_0$. Then, essentially just as before, we can define a non-primitive Selmer group $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$. The Galois group Δ also acts on this object. In the same way as above, we can define the invariant $\lambda(E, \Sigma_0, K)$.

Decomposing $\lambda(E, K)$ and $\lambda(E, \Sigma_0, K)$

If σ is an absolutely irreducible representation of Δ (defined over a sufficiently large finite extension $\mathcal{F}$ of $\mathbf{Q}_p$), then we let $\lambda(E, \sigma)$ denote the multiplicity of σ in $V_E(K_\infty)$. We denote the set of absolutely irreducible representations of Δ by $\mathrm{Irr}(\Delta)$. Then we have the following formula:

$$\lambda(E, K) \;=\; \dim_{\mathbf{Q}_p}\big(V_E(K_\infty)\big) \;=\; \sum_{\sigma} \lambda(E, \sigma)\deg(\sigma) \quad ,$$

where σ varies over $\mathrm{Irr}(\Delta)$.

In the same way as above, we can define the multiplicities $\lambda(E, \Sigma_0, \sigma)$ for all $\sigma \in \mathrm{Irr}(\Delta)$. We have a decomposition

$$\lambda(E, \Sigma_0, K) \;=\; \sum_{\sigma} \lambda(E, \Sigma_0, \sigma)\deg(\sigma) \quad .$$

The difference between $\lambda(E, \Sigma_0, \sigma)$ and $\lambda(E, \sigma)$

In some cases, the set Φ_K is empty. One can then take Σ_0 to be empty. Then we have $\lambda(E, \Sigma_0, \sigma) = \lambda(E, \sigma)$.

In general, just as with the λ-invariants discussed earlier in this talk, one can evaluate the difference $\lambda(E, \Sigma_0, \sigma) - \lambda(E, \sigma)$ in a straightforward way. As before, it can be expressed in the form

$$\lambda(E, \Sigma_0, \sigma) - \lambda(E, \sigma) \;=\; \sum_{\ell \in \Sigma_0} \delta(E, \ell, \sigma) \quad ,$$

a sum over the primes ℓ in Σ_0 where the terms are easily determined integers.

Reducing representations of Δ modulo $\mathfrak{m}$

If ρ is any representation of Δ over $\mathcal{F}$, then one can realize ρ by matrices with coefficients in the integers $\mathcal{O}$ of the local field $\mathcal{F}$. One can then reduce ρ modulo the maximal ideal $\mathfrak{m}$ of $\mathcal{O}$, obtaining a representation $\widetilde{\rho}$ of Δ over the finite field $\mathfrak{f} = \mathcal{O}/\mathfrak{m}$. This finite field has characteristic p. The semisimplification of $\widetilde{\rho}$ will be denoted by $\widetilde{\rho}^{ss}$ and is well-defined.

Suppose that ρ_1 and ρ_2 are two representations of Δ. If p divides $|\Delta|$, then it is possible to have $\widetilde{\rho}_1^{ss} \cong \widetilde{\rho}_2^{ss}$ as representations of Δ over $\mathfrak{f}$ even if $\rho_1 \ncong \rho_2$ as representations of Δ over $\mathcal{F}$. We will think of an isomorphism $\widetilde{\rho}_1^{ss} \cong \widetilde{\rho}_2^{ss}$ as a congruence modulo $\mathfrak{m}$ between the representations ρ_1 and ρ_2.

Congruence relations

Theorem B. *Suppose that Σ_0 is a finite set of primes of* $\mathbf{Q}$ *containing Φ_K, but not containing p. Assume that $\mathrm{Sel}_E(K_\infty)[p]$ is finite. Assume that ρ_1 and ρ_2 are representations of Δ such that $\widetilde{\rho}_1^{ss} \cong \widetilde{\rho}_2^{ss}$. Then 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 $\mathrm{Irr}(\Delta)$ 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.

PGL_2-extensions

As an illustration of the above theorem, suppose that

$$\Delta = \mathrm{Gal}(K/\mathbf{Q}) \cong PGL_2(\mathbf{Z}/p^r\mathbf{Z})$$

for some $r \geq 1$. Then K contains a subfield K_0 such that

$$\Delta_0 = \mathrm{Gal}(K_0/\mathbf{Q}) \cong PGL_2(\mathbf{Z}/p\mathbf{Z}) \quad .$$

It suffices to assume that $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite. This turns out to imply that $\mathrm{Sel}_E(K_\infty)[p]$ is finite.

As a consequence of some results in modular representation theory, one can deduce that all the values of $\lambda(E, \Sigma_0, \sigma)$ as σ varies over $\mathrm{Irr}(\Delta)$ can be determined if one knows the values of $\lambda(E, \Sigma_0, \sigma)$ for σ in $\mathrm{Irr}(\Delta_0)$.

Invariants involving $E(K)$ and $\mathrm{Sel}_E(K)_p$.

One can define some other invariants associated with each $\sigma \in \mathrm{Irr}(\Delta)$. The group $\Delta = \mathrm{Gal}(K/\mathbf{Q})$ also acts on the Mordell-Weil group $E(K)$ and on the p-Selmer group $\mathrm{Sel}_E(K)_p$. Thus, we can define the following two representation spaces for Δ over $\mathbf{Q}_p$:

$$E(K) \otimes_{\mathbf{Z}} \mathbf{Q}_p \quad , \qquad \text{and} \qquad X_E(K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \quad ,$$

where $X_E(K)$ denotes the Pontryagin dual of $\mathrm{Sel}_E(K)_p$.

Define $r(E, \sigma)$ and $s(E, \sigma)$ to be the corresponding multiplicities of σ in these representations space.

Invariants involving $E(K)$ and $\mathrm{Sel}_E(K)_p$.

By definition, one has

$$\mathrm{rank}\big(E(K)\big) \;=\; \sum_{\sigma} \; deg(\sigma) r(E,\sigma) \quad ,$$

and

$$\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(K)_p\big) \;=\; \sum_{\sigma} \; deg(\sigma) s(E,\sigma) \quad ,$$

where σ varies over $\mathrm{Irr}(\Delta)$.

Relationships between the various invariants

One has maps

$$E(K)_{\mathbf{Z}} \otimes (\mathbf{Q}_p/\mathbf{Z}_p) \longrightarrow \mathrm{Sel}_E(K)_p \longrightarrow \mathrm{Sel}_E(K_\infty)_p \quad .$$

The first map is the Kummer map and is injective. The second map is the restriction map and turns out to have finite kernel. One deduces that

$$r(E,\sigma) \;\leq\; s(E,\sigma) \;\leq\; \lambda(E,\sigma)$$

If the Tate-Shafarevich group for E over K is finite, as conjectured, then the first inequality is an equality. However, the second inequality is often strict. Nevertheless, one has the following congruence if the irreducible representation σ is *"orthogonal"*:

$$s(E,\sigma) \;\equiv\; \lambda(E,\sigma) \pmod 2 \quad .$$

The parity conjecture

This refers to the conjecture that the sign in the (conjectural) functional equation for the Hasse-Weil L-function $L(E/K, s)$ is $(-1)^{\mathrm{rank}\left(E(K)\right)}$. A refinement of this conjecture is that if σ is a self-dual irreducible representation of Δ, then the sign in the (conjectural) functional equation for the twisted Hasse-Weil L-function $L(E/F, \sigma, s)$ is $(-1)^{r(E,\sigma)}$. There is a conjectural value for this sign given by Deligne, and spelled out by Rohrlich.

For any prime p, there is a conjecture involving the invariants $s(E, \sigma)$, namely that the conjectural sign in the functional equation for $L(E/F, \sigma, s)$ is $(-1)^{s(E,\sigma)}$. This is a conjecture about the parity of $s(E, \sigma)$, and hence (under suitable assumptions) the parity of $\lambda(E, \sigma)$. We refer to this as the p-Selmer version of the parity conjecture.

Compatibility with congruence relations

With the assumptions in theorem B, and an additional assumption that E has semistable reduction at primes of F lying above 2 and 3, one can show that the parity conjecture is compatible with the congruence relations (viewed as equations over $\mathbf{F}_2$). The proof involves a careful study of the $\delta_v(E,\sigma)$'s.

As an illustration, suppose that $\Delta \cong PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ for $r \geq 0$. Let K_0 be the subfield of K such that $\Delta_0 = \mathrm{Gal}(K_0/F)$ is isomorphic to $PGL_2(\mathbf{F}_p)$. One can show that if $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite, then $\mathrm{Sel}_E(K_\infty)[p]$ is finite too. Thus, it will be enough to assume the finiteness of $\mathrm{Sel}_E(K_{0,\infty})[p]$. Suppose that Σ_0 contains $\Phi_{K/F}$. One then proves the following result.

Corollary. *If the p-Selmer version of the parity conjecture is true for all irreducible representations of Δ_0, then it is also true for all irreducible representations of Δ.*

Other results on the parity conjecture

The p-Selmer version of the parity conjecture has been studied since the 1060s. We can mention papers by B.J. Birch and N. Stephens, by K. Kramer and J. Tunnell, by P. Monsky, by L. Guo, by J. Nekovář, by B.D. Kim, by V. and T. Dokchitser, by J. Coates, T. Fukaya, K. Kato, and R. Sujatha, and by B. Mazur and K. Rubin.

The results in the paper by Coates, Fukaya, Kato, and Sujatha are somewhat parallel to the results just mentioned, although the hypotheses and approach are rather different.

Some recent papers on the parity conjecture

We close by mentioning the most recent papers on this topic.

J. Coates, T. Fukaya, K. Kato, R. Sujatha, *Root numbers, Selmer groups, and non-commutatuve Iwasawa theory*

R. Greenberg, *Iwasawa theory, projective modules, and modular representations*

B. Mazur, K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*

T. Dokchitser, V. Dokchitser, *Regulator constants and the parity conjecture*

Thank you!