A "BASIC NOTIONS" LECTURE ABOUT SIGN INTUITIONS

B. MAZUR

(This is joint work with Karl Rubin)

1. Introduction

As I understand it, a "basic notions" seminar should be about some aspect of mathematics—which can be very elementary, but—which has relevance to the whole of mathematics. Furthermore, Joe Harris tells me that this particular seminar should also give a sample of the type of mathematical question I'm working on at the moment.

So, to try to fulfill both requirements,

- my "basic notion" is the truism that if a subject has more than one facet, one should try to make use of intuitions that are available from the viewpoint, or in the vocabulary of, any one of its facets, to further progress in the other facets.
- the mathematical problem I'm working on, jointly with Karl Rubin, is [*to simply blurt out my entire lecture in one sentence:*] to make use of the very well developed, but almost entirely conjectural, theory of "signs" as computed via local constants in Hasse-Weil L-functions to come up with a theory of parities for ranks of Selmer modules that is entirely *unconditional,* [i.e., proved, dependent upon no conjectures.]

To begin, let me draw this basic triangle on the board

DRAWING OF TRIANGLE WITH VERTICES LABELED
arithmetic, analysis, cohomology

.

Discuss the race between the

- arithmetical
- cohomological
- analytic

aspects of the theory of elliptic curves.

Let $E_{/k}$ be an elliptic curve over a number field k and F/k a finite Galois extension.

To study: the behavior of the arithmetic of E over varying number fields F/k.

The *race* I want to discuss has to do with "parity issues" in the arithmetic and cohomological discussion, corresponding to "sign" issues in the analytic discussion. For certain aspects of the study of elliptic curves one or another of the three facets

Date: February 6, 2006.

(*arithmetic, cohomological, analytic*) are "ahead" of the others and therefore can be used to motivate progress in the "lagging" two facets.

2. On the arithmetic side

The basic arithmetic question connected with an ellipic curve E over a number field F is the **Mordell-Weil group** $E(F)$; that is, the (finitely generated, abelian) group of F-rational points of E. The fundamental numerical invariant of $E(F)$ is the *Mordell-Weil rank*

$$r^{\mathrm{arith}}(E;F) := \dim_{\mathbf{Q}}(E(F)\otimes \mathbf{C}).$$

More delicately, since $E(F)\otimes\mathbf{C}$ is natural a G-representation, we can, for any ($\mathbf{C}$-valued) character τ of a continuous representation of G, also consider

$$r^{\mathrm{arith}}(E;\tau) := \text{the multiplicity of } \tau \text{ in } E(F)\otimes\mathbf{C}.$$

3. On the cohomological side

Here one chooses a prime number p and one forms the p-Selmer module $\mathrm{Sel}_p(E;F)$ that fits into the exact sequence,

$$0 \to E(F)\otimes \mathbf{Q}_p/\mathbf{Z}_p \to \mathrm{Sel}_p(E;F) \to \mathrm{Sha}(E;F)[p^\infty] \to 0,$$

and forms the $\bar{\mathbf{Q}}_p[G]$-module

$$S_p(E;F) := \mathrm{Hom}(\mathbf{Q}_p/\mathbf{Z}_p, \mathrm{Sel}_p(E;F))\otimes_{\mathbf{Z}_p}\bar{\mathbf{Q}}_p.$$

Define the p-**Selmer rank** of E over F to be

$$r_p^{\mathrm{coho}}(E;F) := \dim_{\bar{\mathbf{Q}}_p} S_p(E;F),$$

and also, for any $\bar{\mathbf{Q}}_p$-valued character, τ, of G let

$r_p^{\mathrm{coho}}(E;\tau) :=$ the multiplicity of τ in the G-representation $S_p(E;F)\otimes_{\mathbf{Z}_p}\bar{\mathbf{Q}}_p$.

4. On the analytic side

Let τ now be the character of an irreducible complex valued continuous representation of the Galois group $G = \mathrm{Gal}(F/k)$. The Hasse-Weil L-function $L(E_{/k},\tau;s)$ is defined as a Dirichlet series convergent in an appropriate right-half palne, and is conjectured to have an entire analytic continuation and to satisfy a functional equation of a specific sort:

$$L(E_{/k},\tau;s) = \epsilon(E_{/k},\tau,s)L(E_{/k},\bar{\tau};1-s)$$

where $\epsilon(E_{/k},\tau,s)$ is given as a product of (finitely many, and comparatively elementary) local factors. Moreover,

The order of vanishing of $L(E_{/k},\tau;s)$ at $s=1$ is conjectured to be equal to $r(E,\tau)$.

Let $r^{\mathrm{an}}(E_{/k};\tau)$ denote the order of vanishing of $L(E_{/k},\tau;s)$ at $s=1$.

Sometimes but not always (rarely, in fact) one can actually establish the analytic continuation and functional equation mentioned above. But whether or not this functional equation is proved, one can make perfectly explicit, in many cases, the *expected* $\epsilon(E_{/k}, \tau, s)$ that *should* occur in the functional equation, and also the corresponding local factors.

5. Change of Sign and Parity

We shall be interested in the *parity* of the three versions of *rank* described above, and more specifically, in *changes of parity*. To give vocabulary for this, let τ and τ' be two irreducible representation of the Galois group over k (what the value field of these representations should be will be discussed in a moment) and put:

—

- $\delta^{\mathrm{arith}}(E_{/k}; \tau, \tau') := r^{\mathrm{arith}}(E_{/k}, \tau) - r^{\mathrm{arith}}(E_{/k}, \tau')$ modulo 2,
- $\delta^{\mathrm{an}}(E_{/k}; \tau, \tau') := r^{\mathrm{an}}(E_{/k}, \tau) - r^{\mathrm{an}}(E_{/k}, \tau')$ modulo 2,
- $\delta_p^{\mathrm{coho}}(E_{/k}; \tau, \tau') := r_p^{\mathrm{coho}}(E_{/k}, \tau) - r_p^{\mathrm{coho}}(E_{/k}, \tau')$ modulo 2.

In the first two bullets above, the τ and the τ' are $\mathbf{C}$-valued characters, while in the last bullet they should be taken to be either $\bar{\mathcal{Q}}_p$-valued, or $\mathbf{C}_p$-valued characters.

Nevertheless, it makes sense to formulate the blanket conjecture that all three $\delta(E_{/k}; \tau, \tau')$'s are

(1) independent of the $G_{\mathbf{Q}}$-conjugacy class of the τ and the τ',

and

(2) "equal."

Here (1) is reasonable, given that the $r^{\mathrm{arith}}(E_{/k}; \tau)$ and $r^{\mathrm{arith}}(E_{/k}; \tau')$ count the multiplicities of irreducible representation in a representation defined over $\mathbf{Q}$, allowing (2) to make sense, since although we cannot make a natural identification of irreducible representations defined over $\mathbf{C}$ with those defined over $\bar{\mathbf{Q}}_p$, we can indeed find a natural identification of $G_{\mathbf{Q}}$-conjugacy classes of irreducible representations defined over $\mathbf{C}$ with $G_{\mathbf{Q}}$-conjugacy classes of irreducible representations defined over $\bar{\mathbf{Q}}_p$.

In the race for understanding, you would naively think that δ^{an} lags very much behind the other two quantities, since—at the very least–the other two quantities have a rigorous definition, while the very existence of the quantity δ^{an} depends on the conjectured analytic continuation of L-functions, and this conjecture has been verified in very few cases. Nevertheless ...

6. A semi-local theory for δ^{an}

Things simplify when the character of our $\mathbf{C}$-valued repesentation τ is *real-valued* for then the expected functional equation reads:

$$L(E_{/k}, \tau; s) = \epsilon(E_{/k}, \tau, s) L(E_{/k}, \tau; 2-s)$$

from which we immediately see that the value of the local factor $\epsilon(E_{/k}, \tau, s)$ at $s = 1$ is ± 1. This *sign* is called the *root number* $W(E_{/k}, \tau)$ and governs the parity of the order of vanishing of $L(E_{/k}, \tau; s)$ at $s = 1$: if $W(E_{/k}, \tau) = +1$ then $L(E_{/k}, \tau; s)$ has a zero of even order at $s = 1$. If $W(E_{/k}, \tau) = -1$ then $L(E_{/k}, \tau; s)$ has a zero of odd order, and in particular it is zero, at $s = 1$. For a discussion of root numbers of elliptic curves, see, for example, section 3 of Rohrlich's Compositio article *Galois theory, elliptic curves, and root numbers*, Compositio Mathematica **100** (1996) 311-349.

In discussing the passage from global to local, it is (at least notationally) useful to work with the more general " Galois extensions of étale algebras" as discussed in Bourbaki, rather than considering only Galois field extensions. Specifically, if F/k is our global field extension with Galois group G and if v is a place of k, we will happily work with the étale k_v-algebra $F_v := F \otimes_k k_v$ viewed and F_v/k_v we view as Galois extension with Galois group G. With this understanding, if τ is an irreducible representation of $G = \mathrm{Gal}(F/k)$ we denote by τ_v the very same representation τ, but where we are thinking of G as $\mathrm{Gal}(F_v/k_v)$.

With these conventions, the global root number $W(E_{/k}, \tau)$ is defined as a product of local root numbers almost all of the local factors being $+1$, and all of them being defined in such a way that they are amenable to explicit calculation.

Aside on local constants: The Deligne theory of local constants, over a local field k_v produce "epsilon-factors" $\epsilon(\pi, dx, \psi)$ where π is a representation of the Weil-Deligne group, dx is a Haar measure on K and ψ is an additive character on K^*, where these factors do depend on these auxilary local choices dx and ψ. Rohrlich defines his root number by setting

$$W(E_{/k_v}; \tau, \psi) := \frac{\epsilon(\pi(E, \tau), dx, \psi)}{|\epsilon(\pi, dx, \psi)|}$$

where τ is a given Weil-Deligne representation, and $\pi(E, \tau)$ is defined to be the Weil-Deligne representation that is the tensor product of τ with the Weil-Deligne representation associated to $E_{/k_v}$. This no longer depends upon the choice of dx, but still depends on ψ. [Rohrlich fixes his ψ, though, so he can suppress it from the notation.] Now, however, define for a pair τ, τ' of Deligne-Weil representations with *the same determinant* and real-valued characters the quantity

$$\delta_v^{\mathrm{an}} = \delta_v^{\mathrm{an}}(E_{/k_v}; \tau, \tau') \ \in \ \mathbf{Z}/2\mathbf{Z}$$

by the formula

$$(-1)^{\delta_v^{\mathrm{an}}} \ = \ \frac{W(E_{/k_v}; \tau, \psi)}{W(E_{/k_v}; \tau', \psi)}$$

which makes sense since the RHS is ± 1; and it is well-defined, independent of either dx or ψ.

For any elliptic curve E over a global field k, and for Galois representations τ, τ' of k where τ and τ' have the same determinant and have real-valued characters, we have that $\delta_v^{\mathrm{an}}(E_{/k_v}; \tau_v, \tau_v')$ is defined for all places v, vanishes for all but a finite number of places v of k, and we have the following conjecture.

Conjecture:

$$\delta^{\mathrm{an}}(E_{/k}; \tau, \tau') \ = \ \sum_v \delta_v^{\mathrm{an}}(E_{/k_v}; \tau_v, \tau_v').$$

For fairly general characters τ, τ' over k satisfying the above hypotheses we have explicit formulas allowing us to compute *change of root number, depending upon change of character*. The beauty, here, is that from standard conjectures together with this excursion into the analytic side of things, we get some quite precise expectations regarding how the parity of $r^{\mathrm{an}}(E, K; \tau)$ and therefore $r^{\mathrm{arith}}(E, K; \tau)$ and $r_p(E, K; \tau)$ change (when we pass from one character τ to a different character τ', both of the same determinant and with real-valued characters).

We will refer to the above conjecture as giving us a **semi-local theory** for the change of root number $\delta^{\mathrm{an}}(E_{/k}; \tau, \tau')$.

7. Generalized dihedral field extensions

The type of number field extensions F/k we will have particular interest in is as follows.

The extension F/k is assumed to be Galois, and we also assume that there is a quadratic intermediate extension K/k in F/k (denote by $c \in \mathrm{Gal}(K/k)$ the nontrivial automomorphism). Until further notice $\mathrm{Gal}(F/K)$ will be either a finite abelian p-group (for p an odd prime number) or else an abelian pro-p group. Towards the end of the hour we will be considering more general groups. Letting $G^{\pm} \subset G$ be the $\pm$-eigen-subgroups of the conjugation action of c, and $F^{\pm}/K$ the subfield of F consisting in elements fixed under $G^{\mp}$, we have that F is the composite of F^+ and F^-, and $\mathrm{Gal}(F^{\pm}/K) = G^{\pm}$.

We shall be considering characters over k of the form

$$\eta = \mathrm{Ind}_k^K(\chi)$$

where χ is a Dirichlet character over K. The necessary and sufficient condition for η to be real-valued is that χ be a character belonging to the *minus*-subextension F^-/K. If χ belongs to F^-/K, let us call χ a *minus-character*.

More striking, though, is the fact that—assuming that the conductor of the real-valued character η is relatively prime to the conductor of E—the root numbers $W(E, K; \chi)$ *do not depend on* η. That is,

$$\delta^{\mathrm{an}}(E_{/k}; \eta, \eta') = 0.$$

8. A "cohomological theory" of (relative) local constants

Karl Rubin and I set ourselves the following problem. Working entirely in the cohomological (i.e. "Selmer") facet and working "unconditionally," (i.e., using no outstanding conjectures) we wish to set up the analogue of a semi-local theory of "relative local constants" that performs the same function cohomologically that the theory of local constants perform (conjecturally) for the analytic theory. That is, we have the following program:

(1) For suitable pairs τ_v, τ_v' **define** relative local invariants
$$\delta_{p,v}^{\mathrm{coho}}(E_{/k_v}; \tau_v, \tau_v') \ \in \ \mathbf{Z}/2\mathbf{Z}$$
purely by local cohomological means.
(2) For any elliptic curve E over a global field k, and for suitable pairs τ, τ' prove that $\delta_{p,v}^{\mathrm{coho}}(E_{/k_v}; \tau_v, \tau_v')$ vanishes for all but a finite number of places v of k.
(3) Prove that when the relative local invariants are defined we have the local to global equation
$$\delta^{\mathrm{coho}}(E_{/k}; \tau, \tau') \ = \ \sum_v \delta_{p,v}^{\mathrm{coho}}(E_{/k_v}; \tau_v, \tau_v').$$
(4) Give explicit computations of the relative local invariants.

We feel we have made progress in setting up such a theory in the generalized dihedral context. We fix a quadratic extension of number fields K/k.

(1) **(Local Invariants)** For a place v of K, an elliptic curve E_v/k_v and a local *minus*-Dirichlet character χ_v over K_v we define the *arithmetic (relative) local invariant*
$$\delta_{p,v}^{\mathrm{coho}}(E_v, k_v; \eta_v) \in \mathbf{Z}/2\mathbf{Z}$$
where $\eta = \mathrm{Ind}_k^K(\chi)$ as in the previous section. I'll give the definition in a moment; these $\delta_{p,v}^{\mathrm{coho}}$'s will be "cohomological analogues" of the δ_v^{an}'s we have previously discussed.

We prove, via "visiblity methods," the following

(2) (**Global sign as a sum of local signs**) If E/K is an elliptic curve, and χ, χ' are global Dirichlet *minus*-characters of K, then the corresponding local invariants $\delta_{p,v}^{\mathrm{coho}} = \delta_{p,v}^{\mathrm{coho}}(E/k_v, \eta_v, \eta_v')$ vanish for all but finitely many places v. Moreover, we have the formula
$$\delta^{\mathrm{coho}}(E_{/k}; \eta, \eta') = \sum_v \delta_{p,v}^{\mathrm{coho}}(E/k_v, \eta_v, \eta_v')$$

(3) (**Computability**) The local invariants δ_v^{coho} are reasonably computable, and when we do actually make the computation they conform to the expectations we have using the analytic theory as heuristic.

In particular, we obtain as corollary:

Corollary: Let F^-/K be an abelian p-extension that is a *minus*-extension in the sense defined above and that is unramified at all primes where E has bad reduction and all primes above p split in K/k. If $r_p(E,K)$ is odd, then $r_p(E,F^-) \geq [F^- : K]$.

9. Discussion of previous results

Cornut-Vatsal, Nekovár, Skinner-Urban

10. Definition of the local invariants

In our article, Rubin and I define these invariants in somewhat greater generality, but to get the idea, suppose given an odd prime number p, a local field K_v, an elliptic curve E over K_v, and a cyclic extension L_w/K_v of order a power of p.

By the **Weil trace of E relative to the Galois extension** L_w/K_v, denoted $Tr_{L_w/K_v}(E)$, we mean the abelian variety over K_v of dimension $[L_w : K_v]$ which is characterized functorially as that abelian variety whose group of R-valued points, for any K_v-algebra R, are given by:

$$Tr_{L_w/K_v}(E)(R) := E(R \otimes_{K_v} L_w).$$

There is a natural action of $G = \mathrm{Gal}(L_w/K_v)$ on $E(R \otimes_{K_v} L_w)$ as group of automorphisms and hence on the abelian variety $Tr_{L_w/K_v}(E)$ (over K_v). By the **L_w/K_v-twist of** E we mean the abelian subvariety $A := E_{L_w/K_v}$ defined over K_v of the Weil trace of E,

$$A \subset Tr_{L_w/K_v}(E),$$

that is characterized by the following properties:

- A is stable under the action of G,
- G acts faithfully on A,
- A is a simple abelian variety.

If the order of the cyclic group G is p^ν and R is the unique integral domain quotient of $\mathbf{Z}[G]$ on which G act faithfully, then $R \cong \mathbf{Z}[\zeta_{p^\nu}]$ where ζ_{p^ν} is a primitive p^ν-th root unity. The L_w/K_v-twist of E E_{L_w/K_v} inherits, from the action of G, an action of the ring R as ring of endomorphisms.

Let $\pi = (1 - \zeta_{p^\nu})$. One proves:

$$E[p] = E_{L_w/K_v}[\pi],$$

this equality, of $\mathbf{F}_p$-vector spaces with Galois action, taking place in $Tr_{L_w/K_v}(E)[p]$.

The Kummer cohomology exact sequence for E, coming from

$$0 \to E[p] \to E \xrightarrow{p} E \to 0$$

gives us an $\mathbf{F}_p$-vector subspace,

$$\mathcal{E} := E(K_v)/pE(K_v) \hookrightarrow H^1(K_v, E[p]),$$

and the Kummer cohomology exact sequence for E_{L_w/K_v} coming from

$$0 \to E_{L_w/K_v}[\pi] \to E_{L_w/K_v} \xrightarrow{\pi} E_{L_w/K_v} \to 0$$

gives us an $\mathbf{F}_p$-vector subspace,

$$\mathcal{F} := E_{L_w/K_v}(K_v)/pE_{L_w/K_v}(K_v) \hookrightarrow H^1(K_v, E_{L_w/K_v}[\pi]).$$

Since, by the equality of $\mathbf{F}_p$ vector spaces with Galois action displayed above, we have an equality

$$H^1(K_v, E[p]) = H^1(K_v, E_{L_w/K_v}[\pi])$$

let us denote denote these (equal) $\mathbf{F}_p$-vector spaces by the same letter, $\mathcal{V}$.

Both $\mathcal{E}$ and $\mathcal{F}$ are $\mathbf{F}_p$ vector subspaces of $\mathcal{V}$. Define:

$$\mathcal{D} := \frac{\mathcal{E}}{\mathcal{E} \cap \mathcal{F}}.$$

We define our *local invariant* which is an integer modulo 2 by the formula:

$$\delta_v^{\mathrm{coho}} := \delta_v^{\mathrm{coho}}(E, L_w/K_v) = \dim_{\mathbf{F}_p} \mathcal{D} \mod 2.$$

11. Questions and Conjectures

(1) **Do Euler Systems exist in this generality?** Let $\mathcal{F}/K$ be the maximal pro-p abelian Galois extension of K unramified at primes dividing the conductor of E, and denote by $\mathcal{F}^-/K$ its minus part, relative to the quadratic extension K/k. Our results show that there is sufficiently large Selmer rank to "support" the existence of an Euler system for $(E, \mathcal{F}^-/K)$. Is there, in fact, such an Euler System?

(2) **Large Selmer rank in non-abelian extensions.** Let $\mathcal{K}/K$ be a Galois extension with Galois group a (not necessarily abelian) p-group, and suppose again that it is unramified at primes dividing the conductor of E. Suppose further that $\mathcal{K}/k$ is Galois. By the **minus-degree**, $[\mathcal{K} : K]^-$, of $\mathcal{K}$ over K let us mean the following. Put $G = \mathrm{Gal}(\mathcal{K}/K)$ and $\tilde{G} = \mathrm{Gal}(\mathcal{K}/k)$. Choose an element of order two, $\tilde{c} \in \tilde{G}$ and consider the sub*set* $G^- \subset G$ consisting of elements of G that are brought to their inverse under conjugation by $\tilde{c}$. This set depends upon the choice of $\tilde{c}$ but its cardinality, $|G^-|$, is independent of this choice. Define

$$[\mathcal{K} : K]^- \;=\; |G^-|.$$

Conjecture: Let $\mathcal{K}/K$ be unramified at all primes where E has bad reduction. If $r_p(E, K)$ is odd, then

$$r_p(E, \mathcal{K}) \geq [\mathcal{K} : K]^-.$$