Motives and Diophantine geometry

July 2, 2006

Goals:

I. Understand what a theory of (mixed) motives is expected to do;

II. Understand what it cannot do;

from the viewpoint of Diophantine geometry. And then

III. discuss a proposed remedy:

abelian theory $\rightarrow$ non-abelian theory

homology $\rightarrow$ homotopy

Elementary fact underlying our discussion:

$x \neq y$

$$\Rightarrow \pi_1(X; b, x) \neq \pi_1(X; b, y)$$

Classical expectation:

Variety X

$\rightsquigarrow \zeta(X, s) = \prod L(H^i(X), s)^{(-1)^i} = \cdots$

(zeta-function of X)

$\rightsquigarrow$ Diophantine invariants of X.

Example:

X = Spec(F), $F = \mathbb{Q}(\sqrt{D})$ real quadratic field with discriminant D. Then

$$\zeta(X, s) = \Sigma_m \frac{1}{N(m)^s}$$

as m runs over ideals of F.

But there is a decomposition

$$\zeta(X, s) = \zeta(s) L(\chi_D, s)$$

where

$$L(\chi_D, s) = \Sigma_n \frac{\chi_D(n)}{n^s}$$

and χ_D is the character of the quadratic field computed easily using the Legendre symbol.

Formula for the class number h_X of X:

$$h_X = \frac{\sqrt{D}}{2 \ln u} L(X, 1), \quad D > 0$$

$$h_X = \frac{\epsilon\sqrt{|D|}}{2\pi} L(X, 1), \quad D < 0$$

where u is the fundamental unit of F and ϵ is the number of roots of unity.

Very efficient formula for computing the class number.

Second example:

$E/\mathbb{Q}$ elliptic curve defined by minimal equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Then

$$\zeta(E, s)$$

defined using number of points N_p mod p for almost all primes p, i.e., the number of solutions to this equation in $\mathbf{F}_p$.

Note: Solutions in finite fields are computed readily. But set of rational solutions

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times \text{(finite abelian group)}$$

quite mysterious. For example, when is it infinite, i.e., $r \neq 0$?

Decomposition:

$$\zeta(E,s) = \zeta(s)\zeta(s-1)/L(E,s)$$

where

$$L(E,s) = L_{bad} \prod_{(p,\Delta_E)=1} (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

and $a_p = p - N_p$.

Here, Δ_E is the discriminant of E and L_{bad} is the product of finitely many factors of the form $1/(1 - a_p p^{-s})$ incorporating the primes of bad reduction. Precise definition should go through the Galois action on the *Tate module* of E.

That is, for any prime l, we consider the l^n-torsion subgroups

$$E[l^n]$$

of $E(\bar{\mathbb{Q}})$ which fit into an inverse system

$$\cdots \to E[l^3] \xrightarrow{l} E[l^2] \xrightarrow{l} E[l]$$

The l-adic Tate module of E is defined by

$$T_l E := \varprojlim E[l^n] (\simeq \mathbb{Z}_l^2)$$

and it admits a natural action of

$$\Gamma = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$$

In general, still a difficult action to understand in detail.

We can write

$$L(E,s) = \prod L_p(E,s),$$

an *Euler product*, and $L_p(E,s)$ depends only on the restriction of the action to $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Exact sequence

$$0 \rightarrow I_p \rightarrow \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \rightarrow \mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p) \rightarrow 0$$

so the space of inertia invariants

$$(T_l E)^{I_p}$$

admits an action of

$$\mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p) = < Fr_p >$$

For any $l \neq p$

$$L_p(E,s) = \det([Id - p^{-s}Fr_p]|(T_lE)^{I_p})^{-1}$$

When $(p, \Delta_E) = 1$, I_p-action is trivial, so determinant is of form

$$1 - a_p p^{-s} + b_p p^{-2s}$$

For $p|\Delta_E$, becomes of the form

$$1 - a_p p^{-s}$$

or

$$1$$

The product expression for L converges only for $Re(s)$ large (actually, $Re(s) > 3/2$).

To compute $L(E, s)$ efficiently, use *modular forms*. Among the very non-trivial examples of Langlands' correspondence.

$$L(E, s) = L(f_E, s)$$

'Motivic L-function equals automorphic L-function.'

Proved in this case by Wiles then Breuil-Conrad-Diamond Taylor.

Such an equality endows the motivic L-function with an analytic continuation and a functional equation.

Algorithm:

Find conductor

$$N_E = \prod_{p|\Delta_E} p^{f_p}$$

of E. There is an efficient algorithm for computing f_p using the conductor-discriminant formula of Ogg:

$$f_p = ord_p(\Delta_p) + 1 - c_p$$

where c_p is the number of components in the minimal regular model of E. (Can compute all these quantities using Tate's algorithm.)

Then look for a modular cusp form

$$f_E = \Sigma a_n q^n$$

for $\Gamma_0(N_E)$ of weight two which is a Hecke eigen-new-form determined by the a_p.

With that, we get

$$(2\pi)^s\Gamma(s)L(E,s) = \int_0^\infty f_E(iy)y^{s-1}dy$$

$$= \int_{1/\sqrt{N_E}}^\infty f_E(iy)y^{s-1}dy \pm \int_{1/\sqrt{N_E}}^\infty f_E(iy)y^{1-s}dy$$

convergent for all s.

Conjecture (BSD):

$$ord_{s=1}L(E,s) = \text{rank}E(\mathbb{Q})$$

in particular,

$E(\mathbb{Q})$ is finite iff $L(E,1) \neq 0$.

Known for 'most E' by work of Gross-Zagier and Kolyvagin. More precisely, known for E such that

$$ord_{s=0}L(E,s) \leq 1$$

Such conditions hard to verify computationally.

But can sometimes easily verify

$$L(E,1) = 0.$$

Functional equation:

$$\Lambda(E,s) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$$

satisfies

$$\Lambda(E,s) = w_E\Lambda(E,2-s),$$

where w_E is the *sign of the functional equation*.

Can be computed efficiently using

$$w_E = w_\infty \prod_p w_p$$

and some simple recipes for the local terms.

Thus, when $w_E = -1$,

$$L(E, 1) = 0.$$

If we then verify numerically that

$$L'(E, 1) \neq 0,$$

conclude that $E(\mathbb{Q})$ is infinite, in fact,

$$\simeq \mathbb{Z} \times \text{finite group}$$

That is,

-computation of L-function,

-functional equation,

-and known case of BSD

can sometimes give us complete structure of $E(\mathbb{Q})$.

Even more: In this case, there is an interesting algorithm for using f_E and Heegner points on $X_0(N_E)$ to actually find a point of infinite order on E.

Continuation of BSD: If r is the order of vanishing, then

$$(s-1)^{-r}L(E,s)|_{s=1}$$

$$= |Sha(E)|R_E\Omega \prod_{p|\Delta_E} c_p/|E(\mathbb{Q})(tor)|^2$$

relating L-values to many other *refined arithmetic invariants* of E.

Advice for beginners: Start by spending one day of the week studying each term of the formula (and rest weekends).

Brief discussion of terms.

Important distinction: Rational terms versus transcendental terms.

Rational terms:

$Sha(E)$: The Tate-Shafarevich group of E, conjectured to be finite. Classifies locally trivial torsors for E. Analogous to a class group. (More later.)

$E(\mathbb{Q})(tor)$: (finite) torsion subgroup of $E(\mathbb{Q})$.

c_p: Tamagawa number.

$$c_p = (E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p))$$

Transcendental terms:

R_E: Regulator of E computed using canonical height $<,>$ and basis $\{P_1, P_2, \ldots, P_r\}$ for $E(\mathbb{Q})/E(\mathbb{Q})(tor)$.

$$R_E := |\,\mathrm{det}(< P_i, P_j >)|$$

Thus, R_E is the covolume of the Mordell-Weil group, in a manner analogous to the classical regulator of number fields (covolume of units).

Ω: real period (or 2 times real period)

$$\Omega = \int_{E(\mathbb{R})} |\omega|$$

where

$$\omega = dx/(2y + a_1x + a_3)$$

General principle: L-functions useful for the study of Diophantine problems, in relation to both *general formulas* and *specific techniques*.

In fact, the rough picture for elliptic curves admits a vast generalization.

$X/\mathbb{Q}$ smooth projective variety of dimension d. Then

$$\zeta(X,s) = \prod_i L(H^i(X),s)^{(-1)^i}$$

Each $L(H^i(X),s)$ could decompose further in a natural way.

For example, if $X = \mathrm{Spec}(F)$ where F is a number field Galois over $\mathbb{Q}$, then

$$\zeta(X,s) = L(H^0(X),s) = \prod_\rho L(\rho,s)^{\dim(\rho)}$$

as ρ runs over irreducible representations of $\mathrm{Gal}(F/\mathbb{Q})$ and $L(\rho,s)$ is an Artin L-function.

For $X_0(N)$ modular curve,

$$\zeta(X_0(N), s) = \zeta(s)\zeta(s-1)/L(H^1(X), s)$$

and

$$L(H^1(X), s) = \prod_i L(f_i, s)$$

where the f_i are modular forms of weight 2.

Warning:

Such decompositions are finite-products. Completely different in nature from infinite Euler product decomposition.

In fact, each of the factors themselves admit an Euler product, say,

$$L(f_i, s) = \prod_p L_p(f_i, s) \sim \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

and have the *general analytic shape* of the $L(H^i(X), s)$.

Motives

are the objects of a geometric nature that should account for the natural decomposition of the zeta functions of varieties.

For example, there should be a motive

$$H^i(X).$$

But if

$$L(H^i(X), s) = \prod L_{ij}(s)$$

in a natural way, then should have a natural decomposition

$$H^i(X) = \prod M_{ij}$$

in an abelian category of motives.

Examples:

-Artin motives corresponding to Artin L-functions.

-Motives for modular forms.

-Motives occurring as factors of Shimura varieties.

Analogy:

G: group $\rightsquigarrow$

$\mathbb{Q}[G]$: group algebra living in the linear category of vector spaces with finite group action.

But then

$$\mathbb{Q}[G] \simeq \prod_{\rho} \mathrm{dim}(\rho) V_{\rho}$$

That is, a non-linear object like a group, when put into an appropriate linear category, decomposes naturally.

Similarly, expect an category Mot together with a functor

$$M : Var \rightarrow Mot$$

from the category of varieties, such that for any variety X, a decomposition

$$M(X) \simeq \prod M_i$$

accounts for the decomposition of the zeta function of X.

This way, the natural invariants of X should also 'decompose' enabling us to analyze them piece by piece.

The study of irreducible motives should admit a simplicity analogous to the study of irreducible representations.

For any motive M, expect analytic continuation and functional equation for $L(M, s)$ based upon Langlands' correspondence:

'motivic L-function=automorphic L-function'

generalizing all known examples, e.g., class field theory analysis of abelian Artin L-functions.

Diophantine applications should follows, from general formulas to specific techniques, following the lines of BSD.

Recall: for elliptic curve over $\mathbb{Q}$,

$$ord_{s=1} L(E,s) = \mathrm{rank} E(\mathbb{Q})$$

and

$$(s-1)^{-r} L(E,s)|_{s=1}$$

$$= |Sha(E)| R_E \Omega \prod_{p|\Delta_E} c_p / |E(\mathbb{Q})(tor)|^2$$

Conjectures:

Deligne: generalizes Ω using comparison between algebraic De Rham cohomology and $\mathbb{Q}-$coefficient singular cohomology together with Hodge structure.

Beilinson: generalizes interpretation of order of vanishing and R_E using higher regulator maps from motivic cohomology.

Bloch and Kato: generalize the rational terms.

Next lecture: Some cohomological techniques related to *mixed* motives.