Review of "Euler Systems" by Karl Rubin

Henri Darmon

September 9, 2007

"Euler systems" – a term coined by Kolyvagin in his seminal articles [Ko88a], [Ko88b], and [Ko90] – are the topic of this monograph based on the Hermann Weyl Lectures delivered by the author at the Institute for Advanced Study in 1995. The origins of the Euler System concept can be traced to two independent but almost simultaneous developments:

1. Thaine's "purely cyclotomic" method [Th88] for bounding the exponents of the ideal class groups of cyclotomic fields. The bounds that Thaine obtained were already known thanks to the proof of the Main Conjecture by Mazur and Wiles, in which unramified abelian extensions of cyclotomic fields were constructed from reducible two-dimensional Galois representations occuring in the Jacobians of modular curves. Thaine's method did not rely on modular curves, exploiting instead a norm-compatible system of units in abelian extensions of $\mathbb{Q}$, the so-called *cyclotomic* or *circular* units which had already played a key role in Kummer's investigations of the arithmetic of cyclotomic fields. Thaine's ideas were transposed to great effect by the author of the monograph under review to the context of abelian extensions of imaginary quadratic fields, with the role of the circular units being played by the elliptic units of Siegel and Robert-Ramachandra. In [Ru87], the methods of Coates and Wiles were thus strengthened to give a proof of the finiteness of the Shafarevich-Tate group for complex multiplication elliptic curves with non-vanishing L-series at $s = 1$. This yielded the first examples of elliptic curves whose Shafarevich-Tate groups could be proved to be finite, a breakthrough which dramatically illustrated the power of Thaine's point of view.

2. In Kolyvagin's fundamental articles [Ko88a] and [Ko88b], circular and elliptic units are replaced by certain norm-compatible points on a modular elliptic curve E, the so-called *Heegner points* arising from the theory of complex multiplication. These points are the image under the modular parametrisation $X_0(N) \longrightarrow E$ of points in $X_0(N)$ attached to moduli of elliptic curves with endomorphism ring equal to an order in a quadratic imaginary field K. By the theory of complex multiplication, the Heegner points attached to K are thus defined over certain ring class fields of K. Because of the norm compatibilities that they satisfy, their traces to $E(K)$ generate a subgroup $HP(K)$ of $E(K)$ of rank at most one. (In fact, this rank is 0 unless K satisfies the *Heegner hypothesis* that all primes dividing N are either split or ramified in $K/\mathbb{Q}$.) Kolyvagin shows that if $HP(K)$ is of rank one and $L(E/\mathbb{Q}, 1) \neq 0$, then $E(\mathbb{Q})$ is finite. He also obtains (under the hypothesis of non-triviality of $HP(K)$) bounds on the exponent of the Shafarevich-Tate groups of $E/\mathbb{Q}$ in terms of the index of $HP(K)$ in $E(K)$. In a further article [Ko90], Kolyvagin introduced a remarkable strengthening of his method in which control could be given for the full Mordell-Weil and Shafarevich-Tate groups of E/K, and in which the the order - not just the exponent - of the Shafarevich-Tate group of E could be bounded in terms of the index of $HP(K)$ in $E(K)$. When combined with the important result of Gross and Zagier [GZ] relating the height of a generator of $HP(K)$ to the first derivative of the L-series $L(E/K, s)$ at $s = 1$, this leads to a proof of essentially the entire Birch and Swinnerton-Dyer conjecture for all (modular) elliptic curves $E/\mathbb{Q}$ whose L-function has at most a simple zero at $s = 1$.

It is immediately apparent that the methods of Thaine and Kolyvagin, while applied to different situations, exhibit many formal similarities. The article [Ko90] pointed out the desirability of fitting these arguments into a common axiomatic framework. The monograph under review presents an attempt at formulating such an axiomatisation.

Initially, the idea of an Euler system is perhaps more readily conveyed through an informal discussion covering the range of mathematical phenomena one wishes to axiomatise.

Adopting some of the notations and point of view of Rubin's monograph, let K be a number field, and denote by G_K its absolute Galois group endowed

with the Krull topology. Let V be a finite-dimensional $\mathbb{Q}_p$ vector space endowed with a continuous action of G_K. It is natural to require that V arise "from geometry", say, that it occur in the p-adic étale cohomology of a smooth projective variety over K - a property that is easily checked in all the examples discussed in the monograph under review. This property implies that the action of G_K on V is unramified at almost all primes ℓ, and that the action of the inertia groups at the primes dividing p are potentially semistable in the sense of Fontaine-Mazur.

To such a representation V are attached two types of object: the analytically defined L-function $L(V, s)$, and a Selmer group defined via Galois cohomology. It is the goal the theory of Euler Systems to provide a bridge between these two different types of invariants.

The L-function $L(V, s)$ is defined as a product over the non-archimedean places of K of certain local Euler factors

$$L(V, s) = \prod_v L_v(V, s).$$

If v does not divide p, then the local factor $L_v(V, s)$ is given by

$$L_v(V, s) = \prod_{i=1}^{\dim V^{I_v}} (1 - \alpha_{v,i} Nv^{-s})^{-1},$$

where the $\alpha_{v,i}$ are the eigenvalues of the Frobenius element at v acting on the subspace $V^{I_v} \subset V$ of elements fixed by the inertia group at v, and $Nv \in \mathbb{Z}$ is the norm of v from K to $\mathbb{Q}$. The recipe for defining $L_v(V, s)$ at the primes v dividing p is more subtle, but well understood, at least conjecturally. Known bounds on the eigenvalues $\alpha_{v,i}$ imply that the Euler product defining $L(V, s)$ converges absolutely in a right half plane; for *extremely few* V are the analytic properties of $L(V, s)$ outside this half-plane of convergence understood to any extent. However, it is widely believed that $L(V, s)$ has a meromorphic (and even analytic, if V does not contain the trivial representation as a constituent) continuation to all of $\mathbb{C}$, given by a functional equation whose shape is determined, conjecturally, by the behaviour of the geometric object ("motive") giving rise to V. Even more, it is expected that the special values of $L(V, s)$ at special integer arguments can be expressed as products of complex (typically transcendental) periods attached to V by certain "algebraic

parts" which encode interesting arithmetic information about V. Needless to say, this is far beyond the range of what can be proved for all but the most simple classes of V.

To define the *Selmer group* attached to V over K, first note that the compact group G_K preserves a lattice T in V. Choose such a T, let $A = V/T$ be the torsion group attached to V, and let $V_n = A[p^n]$. It is a free module of rank dim V over $\mathbb{Z}/p^n\mathbb{Z}$ whose isomorphism type as a G_K-module depends only on V if V_1 is irreducible, an assumption that will be made from now on. The p^n-Selmer group $\mathrm{Sel}(K, V_n)$ is a subgroup of $H^1(K, V_n)$ defined by certain local conditions. More precisely, for each place v of K, a subgroup $H^1_f(K_v, V_n) \subset H^1(K_v, V_n)$ is defined, called the *finite part* of the local cohomology group $H^1(K_v, V_n)$. The definition of $H^1_f(K_v, V_n)$ for the primes v dividing p, like that of the local Euler factors in the definition of $L(V, s)$, is somewhat involved; for the purposes of this discussion it will suffice to mention that for the (all but finitely many) places v not dividing p for which I_v acts trivially on V, the group $H^1_f(K_v, V_n)$ is simply made up of *unramified* cohomology classes, which become trivial when restricted to an inertia group at v. The Selmer group $\mathrm{Sel}(K, V_n)$ is the subgroup of classes in the global cohomology group $H^1(K, V_n)$ whose restrictions to $H^1(K_v, V_n)$ belong to $H^1_f(K_v, V_n)$, for all v.

In practice, it is useful to give oneself extra flexibility by allowing the subgroups $H^1_f(K_v, V_n)$ to be defined arbitrarily, subject only to the constraint that, for almost all v, they be equal to the group of unramified cohomology classes. The resulting Selmer group $\mathrm{Sel}(K, V_n)$ of course depends on this choice of subgroups $H^1_f(K_v, V_n) \subset H^1(K_v, V_n)$, even though this choice is customarily suppressed from the notation.

The finiteness of $\mathrm{Sel}(K, V_n)$, for any choice of subgroups $H^1_f(K_v, V_n)$, is an immediate consequence of the theorem of Hermite-Minkowski. Much deeper are the conjectures relating the cardinality of $\mathrm{Sel}(K, V_n)$, and its asymptotic behaviour as $n \longrightarrow \infty$, to the conjectural algebraic parts of special values of $L(V, s)$. Relations of this sort constitute far-reaching generalisations of the analytic class number formula, and provide a conceptual framework in which many important conjectures of number theory (most notably: the Birch and Swinnerton-Dyer conjecture; but also the more general conjectures of Deligne, Beilinson, and Bloch-Kato) can be formulated in a unified setting.

We now describe a general approach for bounding the orders of Selmer groups which is the starting point for all known types of Euler system

arguments. Following a suggestive terminology due to Mazur, the quotient $H_s^1(K_v, V_n) := H^1(K_v, V_n)/H_f^1(K_v, V_n)$ is sometimes called the *singular part* or the *singular quotient* of the local cohomology group $H^1(K_v, V_n)$. If $c \in H^1(K, V_n)$ is a global cohomology class, its natural image in $H_s^1(K_v, V_n)$ is called the *residue* of c at v and denoted $\partial_v(c)$. If c has 0 residue at v, then the image of c in $H^1(K_v, V_n)$ belongs to $H_f^1(K_v, V_n)$ and is then called the *value* of c at v.

Of crucial importance is the notion of a *dual Selmer group* attached to $\mathrm{Sel}(K, V_n)$. To begin, let $V_n^* := \hom(V_n, \mu_{p^n})$ denote the *Kummer dual* of V_n, equipped with its natural G_K-action. Tate showed that the cup-product pairing composed with the identification of local class field theory:

$$H^1(K_v, V_n) \times H^1(K_v, V_n^*) \longrightarrow H^2(K_v, \mu_{p^n}) = \mathbb{Z}/p^n\mathbb{Z}$$

is non-degenerate. Also, if I_v acts trivially on V_n and v does not divide p, then the groups of unramified cohomology classes in $H^1(K_v, V_n)$ and $H^1(K_v, V_n^*)$ are exact annihilators of each other. *Defining* $H_f^1(K_v, V_n^*)$ to be the annihilator of $H_f^1(K_v, V_n)$ under the local Tate pairing yields the definition of the *dual Selmer group* $\mathrm{Sel}(K, V_n^*) \subset H^1(K, V_n^*)$ attached to $\mathrm{Sel}(K, V_n)$.

The global duality theorem for Selmer groups states that, while the orders of $\mathrm{Sel}(K, V_n)$ and $\mathrm{Sel}(K, V_n^*)$ are subtle invariants about which one knows very little a priori, the ratio of these orders is equal to product of simple local terms which in practice can be calculated without much difficulty. More precisely, one has (cf. for example [DDT], thm. 2.19)

$$\frac{\#\mathrm{Sel}(K, V_n)}{\#\mathrm{Sel}(K, V_n^*)} = \frac{\#H^0(K, V_n)}{\#H^0(K, V_n^*)} \prod_v \frac{\#H_f^1(K_v, V_n)}{\#H^0(K_v, V_n)} =: \chi(K, V_n). \qquad (1)$$

Motivated by the analogy between equation (1) and the Riemann-Roch formula, let us call the easily computable number $\chi(K, V_n)$ the *Euler characteristic* attached to $\mathrm{Sel}(K, V_n)$.

Let S be any finite set of primes of K. The *relaxed Selmer group* $\mathrm{Sel}(K, V_n)_{(S)}$ is defined by suppressing the local conditions at the primes of S: namely, $\mathrm{Sel}(K, V_n)_{(S)}$ is the set of classes in $H^1(K, V_n)$ which belong to $H_f^1(K_v, V_n)$ for all places $v \notin S$, and satisfy no further conditions at the places $v \in S$. The *restricted* Selmer group $\mathrm{Sel}(K, V_n^*)_{[S]}$ is defined to be the set of classes in $\mathrm{Sel}(K, V_n^*)$ whose value at v is 0, for all $v \in S$. It is clear that $\mathrm{Sel}(K, V_n)_{(S)}$ and $\mathrm{Sel}(K, V_n^*)_{[S]}$ are dual Selmer groups in the sense described above, so

that, applying the duality theorem once more and comparing it with formula (1) yields the useful identity:

$$\frac{\#\mathrm{Sel}(K, V_n)_{(S)}}{\#\mathrm{Sel}(K, V_n^*)_{[S]}} = \chi(K, V_n) \prod_{v \in S} \#H_s^1(K_v, V_n). \qquad (2)$$

This identity is exploited in conjunction with the tautological exact sequence

$$0 \longrightarrow \mathrm{Sel}(K, V_n) \longrightarrow \mathrm{Sel}(K, V_n)_{(S)} \xrightarrow{\partial_S} \oplus_{v \in S} H_s^1(K_v, V_n). \qquad (3)$$

More precisely, a set of primes S as above is said to *control* the Selmer group $\mathrm{Sel}(K, V_n^*)$ if $\mathrm{Sel}(K, V_n^*)_{[S]}$ is trivial, ie., if the natural map obtained by restriction

$$\mathrm{Sel}(K, V_n^*) \longrightarrow \oplus_{v \in S} H^1(K_v, V_n^*)$$

is injective. The Chebotarev density theorem can often be used to produce an abundance of finite sets S which control $\mathrm{Sel}(K, V_n^*)$. Suppose now that S is a set of primes which controls $\mathrm{Sel}(K, V_n^*)$, and, for simplicity, that $\chi(K, V_n) = 1$. Then the identity (2) shows that the two groups appearing on the right of the exact sequence (3) have the same cardinality. Hence, the problem of bounding the size of $\mathrm{Sel}(K, V_n)$ - the kernel of the residue map ∂_S - becomes equivalent to that of bounding the size of the cokernel of ∂_S. Thus is the main problem transformed into one of *constructing* a sufficiently large supply of classes in the relaxed Selmer group $\mathrm{Sel}(K, V_n)_{(S)}$ whose residues can be controlled explicitly and related to L-function behaviour. This simple idea is at the root of all Euler system arguments, and leads to the following tentative "working definition" of an Euler system.

Informal definition An *Euler system* attached to (K, V_n) is the data of

1. A system of finite collections of primes of K which control the Selmer group $\mathrm{Sel}(K, V_n^*)$;

2. For each set S in this system, an explicitly constructible subgroup

$$X_S \subset \mathrm{Sel}(K, V_n)_{(S)};$$

3. A relationship between the index of $\partial_S(X_S)$ in $\oplus_{v \in S} H_s^1(K_v, V_n)$ and algebraic parts of special values of $L(V, s)$.

This informal definition is of course too vague to be made into a precise mathematical one, and thus falls far short of the goals set for himself by the

author of the monograph under review. But it is worth pointing out that Euler systems (in the above vaguely defined sense) have cropped up in a rich variety of guises and played key roles in many of the important number theoretic breakthroughs of the last decades. To mention only the most salient examples:

1. The Euler systems of Gauss sums and of circular units, used [Ko90], [Ru89], [Ru90] to control the minus and plus parts respectively of ideal class groups of cyclotomic fields. In this setting, one may take $K = \mathbb{Q}$, and V a twist by a Dirichlet character of the p-adic representation $\mathbb{Q}_p(1)$ describing the action of $G_{\mathbb{Q}}$ on the p-power roots of unity. The subgroup $X_S \subset H^1(\mathbb{Q}, V_n)$ is constructed from the images of certain Gauss sums or circular units under the Kummer map.

2. The Euler system of elliptic units, exploited (as mentionned earlier) by Rubin to prove the finiteness of the Shafarevich-Tate group of elliptic curves with complex multiplication with non-vanishing L-series at $s = 1$. This Euler system, which controls the size of ideal class groups of abelian extensions of imaginary quadratic fields, also allowed the proof of the two-variable main conjecture for imaginary quadratic fields [Ru91], which in the cyclotomic setting had been established earlier by Mazur and Wiles.

3. In Kolyvagin's Euler system of Heegner points, the field K is a quadratic imaginary field, and the representation V is equal to $T_p(E) \otimes \mathbb{Q}_p$, where $T_p(E)$ is the p-adic Tate module of a (modular) elliptic curve over $\mathbb{Q}$. The classes in $\mathrm{Sel}(K, V_n)_{(S)}$ are constructed by taking the image under the Kummer map of suitable combinations of Heegner points (the so-called "Kolyvagin derivatives", which also appear in the constructions of examples 1 and 2) defined over the ring class field K_S of K of conductor equal to the product of the primes in S. A priori, these classes belong only to $H^1(K_S, V_n)$, but are invariant under the action of $\mathrm{Gal}(K_S/K)$, so that they "descend" to classes defined over K, once suitable technical conditions are imposed. For p large enough, Kolyvagin is able to produce a set S of primes which controls $\mathrm{Sel}(K, V_n)$ (note that in this setting $V_n = V_n^*$, because of the Weil pairing) and for which the index of $\partial_S(X_S)$ in $\oplus_{v \in S} H^1_f(K_v, V_n)$ is equal to p^{n+t}, where p^t is the maximal power of p which divides the basic Heegner point

7

$P_K \in E(K)$ (the generator of $HP(K)$). The relation between this index and special values of L-series is supplied by the analytic formula of Gross and Zagier [GZ]. Kolyvagin's Euler system of Heegner points can be generalised to the setting of elliptic curves over totally real fields [KL]. The role of modular curves is played in this context by Shimura curves which are equipped with a similar supply of Heegner points. The Gross-Zagier formula has been extended to this setting in [Zh01].

4. Closely related to Kolyvagin's Euler system is the Euler system attached to Heegner cycles on the Chow groups of Kuga-Sato varieties, exploited by Nekovar to control the Selmer groups attached to modular forms of higher even weight. (See [Ne92], and [Zh97].)

5. Flach's Euler system [Fl], where $K = \mathbb{Q}$ and $V = \mathrm{Sym}^2(T_p(E)) \otimes \mathbb{Q}_p$, the symmetric square representation attached to a modular elliptic curve (or a modular form of weight 2, more generally). Flach's cohomology classes in X_S are constructed using algebraic K-theory from cycles in the product of two modular curves: the key geometric ingredient in this delicate and beautiful construction are certain remarkable units in the field of functions of the (affine) modular curves, the so-called *modular units*. The groups of explicit cohomology classes X_S that Flach constructs enable him to bound the exponent (but not the order) of the Selmer group of the symmetric square representation attached to E, in terms of the associated L-value.

6. In [W] and [TW], a different approach is followed to bound the size of the Selmer group of the symmetric square. In some sense, the approach is dual to Flach's, since here the representation V is the adjoint of $T_p(E)$, which is the Kummer dual of the Symmetric square representation. The group X_S in the Taylor-Wiles argument is constructed from p-adic deformations of the representation $T_p(E)$ arising from modular forms. The method actually produces an upper bound on the order, and not merely the exponent of the Selmer group attached to V. In addition to providing more evidence for the general Bloch-Kato conjectures, the method of Taylor-Wiles (suitably generalised to two-dimensional Galois representations arising from weight two modular forms) has a striking application to proving the isomorphism between certain Hecke rings and deformation rings, and thereby establishing the

Shimura-Taniyama-Weil conjecture for all (semistable, a technical condition that has subsequently been removed) elliptic curves over $\mathbb{Q}$. The Taylor-Wiles approach enjoys another advantage over Flach's Euler system: since it does not rely on modular units it generalises more readily to elliptic curves (or modular forms) over totally real fields, where the role of modular curves must now be played by Shimura curves which are not equipped with a collection of cusps.

7. Returning to the case where $V = T_p(E) \otimes \mathbb{Q}_p$, but where now $K = \mathbb{Q}$, Kato has introduced [Sch] a novel method for constructing an Euler system of classes in $H^1(\mathbb{Q}, V_n)_{(S)}$. These classes are constructed from the so-called *Beilinson elements* in the K^2 of the modular function field constructed from modular units, and are in fact obtained by twisting this construction of Beilinson. Kato's method yields information about the arithmetic of Mordell-Weil groups over cyclotomic fields that is not accessible through Kolyvagin's method; on the other hand, it reveals less about elliptic curves over $\mathbb{Q}$ of analytic rank one. Like Flach's Euler system, the Euler system of Kato makes a crucial use of modular units, and hence does not generalise in any obvious way to other number fields such as totally real fields.

The motivation for abstracting the common features of all the examples discussed above should be apparent. To arrive at such a mathematically rigourous yet sufficiently malleable definition of Euler system is the main goal of the monograph under review. The author proposes a definite set of axioms for an Euler system, and is able to prove a result bounding the order of a Selmer group in terms of the behaviour of this object. The gain in precision, allowing the formulation and proof of a precise theorem, is offset by a certain loss of generality: the axioms in the monograph are sufficient to capture the Euler systems of Gauss sums and circular units, as well as Kato's Euler system, but none of the others. The author explains how his axioms can be amended or relaxed to include some of the other examples of Euler systems, such as the important Euler system of Heegner points.

Written by one of the major contributors to the subject, Rubin's monograph is recommended as a companion to the more elementary and thus more accessible texts such as [Gr] for those who wish to learn about this fascinating and still poorly understood area of number theory which is sure to remain a focus of intense research activity in the years to come.

References

[DDT] Darmon, Henri; Diamond, Fred; Taylor, Richard. *Fermat's last theorem.* Elliptic curves, modular forms and Fermat's last theorem (Hong Kong, 1993), 2–140, Internat. Press, Cambridge, MA, 1997.

[Fl] Flach, Matthias. *A finiteness theorem for the symmetric square of an elliptic curve.* Invent. Math. **109** (1992), no. 2, 307–327.

[Gr] Gross, Benedict H. *Kolyvagin's work on modular elliptic curves.* L-functions and arithmetic (Durham, 1989), 235–256, London Math. Soc. Lecture Note Ser., **153**, Cambridge Univ. Press, Cambridge, 1991.

[GZ] Gross, Benedict H.; Zagier, Don B. *Heegner points and derivatives of L-series.* Invent. Math. **84** (1986), no. 2, 225–320.

[Ko88a] Kolyvagin, V. A. *The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 6,1154–1180, 1327 translation in Math. USSR-Izv. **33** (1989), no. 3, 473–499.

[Ko88b] Kolyvagin, V. A. *Finiteness of $E(\mathbb{Q})$ and $\underline{III}(E, \mathbb{Q})$ for a subclass of Weil curves.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3,522–540, 670–671 translation in Math. USSR-Izv. 32 (1989), no. 3, 523–541.

[Ko90] Kolyvagin, V. A. *Euler systems.* The Grothendieck Festschrift, Vol. II, 435–483, Progr. Math., **87**, Birkhäuser Boston, Boston, MA, 1990.

[KL] Kolyvagin, V. A.; Logachev, D. Yu. *Finiteness of $\underline{III}$ over totally real fields.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 55 (1991), no. 4,851–876 translation in Math. USSR-Izv. 39 (1992), no. 1, 829–853

[Ne92] Nekovár, Jan. *Kolyvagin's method for Chow groups of Kuga-Sato varieties.* Invent. Math. **107** (1992), no. 1, 99–125.

[Ru87] Rubin, Karl. *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication.* Invent. Math. **89** (1987), no. 3, 527–559.

[Ru89] Rubin, Karl. *Kolyvagin's system of Gauss sums.* Arithmetic algebraic geometry (Texel, 1989), 309–324, Progr. Math., **89**, Birkhäuser Boston, Boston, MA, 1991.

[Ru90] Rubin, Karl. Appendix, in Lang, Serge Cyclotomic fields I and II. Combined second edition. Graduate Texts in Mathematics, **121**. Springer-Verlag, New York, 1990.

[Ru91] Rubin, Karl. *The "main conjectures" of Iwasawa theory for imaginary quadratic fields.* Invent. Math. **103** (1991), no. 1, 25–68.

[Sch] Scholl, A. J. *An introduction to Kato's Euler systems.* Galois representations in arithmetic algebraic geometry (Durham, 1996), 379–460, London Math. Soc. Lecture Note Ser., 254, Cambridge Univ. Press, Cambridge, 1998.

[Th88] Thaine, Francisco. *On the ideal class groups of real abelian number fields.* Ann. of Math. (2) **128** (1988), no. 1, 1–18.

[TW] Taylor, Richard; Wiles, Andrew. *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) **141** (1995), no. 3, 553–572.

[W] Wiles, Andrew. *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) **141** (1995), no. 3, 443–551.

[Zh97] Zhang, Shouwu. *Heights of Heegner cycles and derivatives of L-series.* Invent. Math. bf 130 (1997), no. 1, 99–152.

[Zh01] Zhang, Shouwu Heights of Heegner points on Shimura curves. Ann. of Math. (2) **153** (2001), no. 1, 27–147.