B. MAZUR

Modular Curves and Arithmetic

Introduction

The real number

\[
\frac{\sin \frac{2\pi}{13} \cdot \sin \frac{5\pi}{13} \cdot \sin \frac{6\pi}{13}}{\sin \frac{\pi}{13} \cdot \sin \frac{3\pi}{13} \cdot \sin \frac{4\pi}{13}}
\]

is a (fundamental) unit in the field \( \mathbb{Q}(\sqrt{13}) \). It has been known since 1837 that one can systematically produce units in real quadratic fields (and hence produce solutions of Pell’s equation) by trigonometric expressions of the above sort.\(^1\)

More generally, the circular units, i.e., Norms of

\[
\frac{1 - \frac{2\pi i a}{N}}{1 - \frac{2\pi i}{N}}
\]

for relatively prime integers \( a \) and \( N \), generate subgroups of finite index in the group of units of number fields \( F \) which are abelian over \( \mathbb{Q} \). The interest in circular units stems from the fact that they are “sufficiently many” explicitly constructed units, and also from the fact that their “position” in the full group of global units (and in certain groups of local units) bears upon deep arithmetic questions concerning \( F \).

\(^1\) The discoverer of this method \([11]\) remarks that it is far less efficient for numerical calculation than is the method of continued fractions (a sentiment we may easily share by considering the displayed example above) and he rather envisions it “comme un rapprochement entre deux branches de la science des nombres”.

[185]
By the work of [48], [49], [66]–[69], [60], we now have an analogous set-up for number fields which are abelian extensions of quadratic imaginary fields (the theory of elliptic units).

It has long been observed that there are resonances between the question of determining the group of units in a number field, and that of determining the group of rational points of an elliptic curve $E$ over a number field. If $K$ is a number field, the theorem of Mordell–Weil asserts that $E(K)$, the group of $K$-rational points of $E$, is finitely generated.

The problem of producing by some systematic means, sufficiently many explicitly constructed rational points in the Mordell–Weil group $E(K)$ seems, however, to be hampered from the outset by the fact that, in contrast to the problem of units, the rank of $E(K)$ is an erratic function of $K$ about which we know little.

Nevertheless, thanks to recent work of Coates–Wiles, Rubin, Greenberg, Gross–Zagier and Rohrlich, a fascinating picture is emerging in the study of the Mordell–Weil group of elliptic curves, which reminds one of the already established theory of elliptic units. The general problem encompassing this recent work is that of understanding, for $E/Q$ an elliptic curve over $Q$, the behavior of the Mordell–Weil group $E(L)$ where $L$ is a (varying) abelian extension of a (fixed) quadratic imaginary number field. In these Mordell–Weil groups one can produce an "orderly" and systematic supply of rational points (Heegner points). The Heegner points do not always account for the full rank of the Mordell–Weil group, but, in some statistical sense, yet to be made precise, they may very well provide the major contribution (the "dominant term") whose asymptotic nature is succinctly describable. In consequence, the erratic nature of the rank of $E(L)$ for varying $L$ would be due to the presence of an "error term" whose fluctuations would be, perhaps, truly difficult to come to grips with, but nevertheless comparatively minor in amplitude.

Since it is usually sound mathematical practice to deal with dominant terms, before getting down to error terms, this deserves close study. What makes this study even more attractive is the recent development of new tools which might be brought to bear on these problems ($p$-adic heights; two-variable $p$-adic $L$ functions, and a number of novel approaches to the handling of special values of classical $L$ functions).

The object of this expository paper is to sketch the "emerging picture" much of which is still conjectural, and to describe recent advances towards its development.

---

2 Which is assumed to admit a parametrization by modular functions.
I. Arithmetic

1. Weil parametrizations. The Weil–Taniyama conjecture asserts that any elliptic curve over \( \mathbb{Q} \) can be parametrized by one of the family of modular curves \( X_0(N) \), for \( N = 1, 2, \ldots \). Recall that the modular curve \( X_0(N)/\mathbb{Q} \) is Shimura’s canonical model of the Riemann surface \( \mathcal{H}/\Gamma_0(N) \), the quotient of the upper half-plane by the action of the subgroup \( \Gamma_0(N) \) consisting of matrices \( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \) in \( \text{SL}_2(\mathbb{Z}) \) with \( c \equiv 0 \mod N \).

It has been abundantly clear for years that one has a much more tenacious hold on the arithmetic of an elliptic curve \( E/\mathbb{Q} \) if one supposes that it is so parametrized. We will suppose so, and, moreover, with no loss of generality, we suppose that we have a Weil parametrization: a non-trivial morphism \( \varphi: X_0(N) \rightarrow E \) defined over \( \mathbb{Q} \) which brings the holomorphic differential on \( E \) to a new form, and which brings the cusp \( \infty \) to the origin in \( E \). The integer \( N \) for which this holds is an isogeny-class invariant of \( E \), called the conductor of \( E \). See [40] for tables listing quantities of elliptic curves possessing Weil parametrizations. Any complex multiplication elliptic curve over \( \mathbb{Q} \) admits a Weil parametrization.

Remark. If \( E \) admits a Weil parametrization by \( X_0(N) \) and if \( d \) is a divisor of \( N \) which is the product of an even number of distinct primes, and is relatively prime to \( N/d \), then by the work of Ribet and Jacquet-Langlands, \( E \) also admits a parametrization by a certain “Shimura curve” attached to the quaternion algebra over \( \mathbb{Q} \) which is nonsplit at the prime divisors of \( d \).

For a more comprehensive study of “Heegner points” (cf. Section 4 below) on \( E \), it may be useful to deal with the entire assortment of Shimura curve parametrizations of \( E \), and not only its Weil parametrization.

2. Mordell–Weil rank. Let \( L/K \) be a finite abelian extension of number fields and \( E/K \) an elliptic curve over \( K \). By the Mordell–Weil theorem \( E(L) \) is finitely generated. We may decompose the complex vector space \( E(L) \otimes \mathbb{C} \) as a direct sum:

\[
E(L) \otimes \mathbb{C} = \bigoplus \nabla(E, \chi)
\]

where \( \chi: \text{Gal}(L/K) \rightarrow \mathbb{C} \) ranges through all characters, and \( \nabla(E, \chi) \) is the \( \chi \)-eigensubspace in \( E(L) \otimes \mathbb{C} \). The classical canonical normalized

---

3 For an exposition of this theory, see Chapter IV of [34].
height pairing $\langle \cdot, \cdot \rangle$ gives $E(L) \otimes \mathbb{C}$ and each $V(E, \chi)$ a nondegenerate Hermitian structure. Let $r(E, L)$ denote the rank of $E(L)$ and $r(E, \chi)$ the complex dimension of $V(E, \chi)$.

One has hardly begun to achieve significant understanding of the asymptotics of the function

$$\chi \mapsto r(E, \chi)$$

for fixed $E/K$. Two restricted types of “variation of $\chi$” come to mind: horizontal variation, where one allows $\chi$ to run through all characters of fixed order, and vertical variation, where one considers all characters whose conductors have prime divisors belonging to a fixed, finite, set of primes $S$.

In a series of papers ([14]–[16]), Goldfeld and co-authors have considered the problem of horizontal variation for quadratic characters $\chi$, where $K = \mathbb{Q}$. Goldfeld conjectures that the “average value of $r(E, \chi)$” is $1/2$. This is consistent with the partial results he has obtained, the most striking being his theorem with Hoffstein and Patterson which implies that, when $E/Q$ has complex multiplication, there are an infinity of quadratic $\chi$ over $\mathbb{Q}$ such that $r(E, \chi) = 0$. The conjecture is also in accord with the qualitative results that are being obtained in the case of “vertical variation”; namely, that the bulk of the contribution to the Mordell–Weil rank over abelian extensions of quadratic number fields is of a size that would be given by the most conservative estimate compatible with the parity restrictions forced by the functional equation of associated $L$ functions, via the conjectures of Birch and Swinnerton-Dyer. It would be interesting to experiment further with “horizontal variation” (e.g., cubic characters) to get a broader view.

3. Anti-cyclotomic extensions. Let $k \subseteq \mathbb{C}$ be a quadratic imaginary field. An anti-cyclotomic extension of $k$ is a finite abelian extension $L/k$ such that $L/Q$ is a Galois extension, whose Galois group is a generalized dihedral group in the following sense: there is an involution $\sigma$ of $L$ which induces complex conjugation on $k$, and such that for every $g \in \text{Gal}(L/k)$ we have $\sigma g \sigma^{-1} = g^{-1}$. An anti-cyclotomic character of $k$ is a continuous homomorphism of $\text{Gal}(\bar{k}/k)$ to $\mathbb{C}^*$ whose $k/Q$ conjugate is equal to its inverse. Thus

---

4 For more general results concerning the nonvanishing of the $L$ function of modular forms twisted by quadratic characters evaluated at the center of the critical strip, see § 9 below, Waldspurger [63], and the exposition of Waldspurger's results in [62].
the anti-cyclotomic extensions of $k$ are precisely those abelian extensions of $k$ all of whose associated characters are anti-cyclotomic.

Examples of anti-cyclotomic extensions are given by ring-class fields over $k$: Recall that for every positive number $c$, the order of conductor $c$, $\mathcal{O}_c$, in the full ring of integers $\mathcal{O}$ of $k$ is the module $\mathbb{Z} + c \cdot \mathcal{O}$, immediately seen to be a subring of $\mathcal{O}$ of finite index. Viewing $\mathcal{O}_c \subset \mathcal{O} \subset k \subset \mathbb{C}$ as a lattice in the complex plane, and viewing the elliptic modular function $j$ as a function of lattices, one shows that $j(\mathcal{O}_c)$ is a real algebraic number. One defines $H_c$, the ring class field of $k$ of conductor $c$, to be $k(j(\mathcal{O}_c)) \subset \mathbb{C}$. Class field theory establishes an isomorphism of groups

$$\text{Gal}(H_c/k) \cong \text{Pic}(\mathcal{O}_c)$$

where $\text{Pic}(\mathcal{O}_c)$ denotes the group of invertible $\mathcal{O}_c$-ideal classes. Taking our involution $\sigma$ to be the automorphism of $H_c$ induced by complex conjugation, one sees that $H_c$ is an anti-cyclotomic extension of $k$. Moreover, any anti-cyclotomic extension of $k$ is contained in a ring-class field $H_c$ for some $c$. If $\chi$ is an anti-cyclotomic character of $k$, and $c$ is the minimal integer for which $\chi$ belongs to $H_c$ then $\chi$ is said to be primitive on $H_c$.

A character $\chi$ on $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is anti-cyclotomic when restricted to $\text{Gal}(k/k)$ if and only if $\chi$ is quadratic.

4. **Heegner points.** These points were first discovered by Heegner [25] and developed by Birch [4], [5]. They may be now seen as a particular case of a quite general construction ("special points and cycles") on Shimura varieties. Heegner points call attention to themselves by virtue of their being a plentiful and orderly supply of points on modular curves $X_0(N)$ rational over anti-cyclotomic extensions of quadratic number fields. Given a Weil parametrization $\varphi : X_0(N) \to E$, the image of the Heegner points will generate some portion of the Mordell–Weil group of $E$. The marvelous result of Gross–Zagier gives us some idea of the portion generated. We sketch the definition of Heegner points.

If $K$ is a field of characteristic 0, a pair $(\mathfrak{E}, \mathcal{O}_N)$ consisting of an elliptic curve $\mathfrak{E}$ over $K$, and a cyclic subgroup of order $N$, $\mathcal{O}_N \subset \mathfrak{E}$, rational over $K$ defines a $K$-valued point of $X_0(N)$, which we shall denote $j(\mathfrak{E}, \mathcal{O}_N)$.

---

5 We restrict ourselves here to Heegner points on $E$ arising from its Weil parametrization. This accounts for the restrictedness of the Heegner Hypothesis below.

As hinted in Section 1, it will be eventually necessary to consider the Heegner points of $E$ arising from its various Shimura curve parametrization as well. For this theory, see [28], especially Chapter 3.
Now let \( \mathcal{O} \) denote a quadratic imaginary field contained in \( \mathbb{C} \), \( \mathcal{O} \) an order of conductor \( c > 0 \) contained in the ring of integers of \( \mathcal{O} \).

**Heegner Hypothesis.** We say that the pair \((\mathcal{O}, N)\) satisfies the Heegner Hypothesis if there exists an invertible \( \mathcal{O} \)-ideal \( \mathcal{N} \subset \mathcal{O} \) such that \( \mathcal{O}/\mathcal{N} \) is cyclic of order \( N \).

This is the case when, for example, \( N \) is prime to the discriminant of \( \mathcal{O} \), and every prime dividing \( \mathcal{N} \) splits in the ring of integers of \( \mathcal{O} \). Suppose now, that \((\mathcal{O}, \mathcal{N})\) satisfies the Heegner hypothesis and choose an ideal \( \mathcal{N} \) as above.

Let \( y(\mathcal{O}, \mathcal{N}) \) denote the point \( j(\mathcal{O}/\mathcal{O}, \mathcal{N}^{-1}/\mathcal{O}) \) in \( X_0(N)(\mathbb{C}) \). One learns from the classical theory of complex multiplication that \( y(\mathcal{O}, \mathcal{N}) \) is defined over the field \( \mathbb{H} \subset \mathbb{C} \), and its full set of Galois-conjugates over \( \mathcal{O} \) is operated on principally and transitively by \( \text{Gal}(\mathcal{H}/\mathcal{K}) \). We refer to \( y(\mathcal{O}, \mathcal{N}) \) or any of its Galois-conjugates as basic Heegner points (of type \((\mathcal{O}, \mathcal{N})\)).

Let \( w(\mathcal{O}, \mathcal{N}) \) denote the image of \( y(\mathcal{O}, \mathcal{N}) \) under the Weil parametrization \( \varphi \), in the Mordell–Weil group of \( E \) over \( \mathcal{H} \). We refer to the \( w(\mathcal{O}, \mathcal{N}) \) and their Galois-conjugates as basic Heegner points on \( E \).

If \( \chi \) is a primitive character on \( \text{Gal}(\mathcal{H}/\mathcal{K}) \), define

\[
\omega(\chi, \mathcal{N}) = \sum \chi^{-1}(g) \cdot w(\mathcal{O}, \mathcal{N})^g \in V(\chi).
\]

One easily sees that, up to sign, \( w(\chi, \mathcal{N}) \) is independent of the choice of \( \mathcal{N} \), and hence depends only upon \( \chi \).

We shall say that the pair \((\mathcal{O}, E)\) satisfies the Heegner hypothesis (for the Weil parametrization) if the pair \((\mathcal{O}, N)\) satisfies the Heegner hypothesis, as above.

**II. The (\( \mathbb{C} \)-valued) analytic theory**

5. *L* functions. Let \( E \) be a Weil curve, i.e., \( E \) is an elliptic curve admitting a parametrization by \( X_0(N)(\mathbb{Q}) \) over \( \mathbb{Q} \) as in Section 1.

Let \( \mathcal{O} \) be a quadratic imaginary field, \( \chi \) a finite Hecke character for \( \mathcal{O} \) of conductor \( f \) with values in \( \mathbb{C} \). If \( v \) is a valuation of \( \mathcal{O} \), let \( \chi_v \) denote the \( v \)-adic component of \( \chi \).

The *Euler factor* \( L_v(E/\mathcal{O}, \chi_v, s) = L_v \) is defined for places \( v \mid N \cdot f \cdot \infty \) by the formula:

\[
L_v^{-1} = 1 - \chi_v(\pi_v)Nv^{-s} + \chi_v^2(\pi_v)Nv^{1-2s}.
\]
where \( N_v \) is the cardinality of \( k(v) \), the residue field of \( v \), \( \pi_v \) is a \( v \)-adic uniformizer, and \( a_v \) is that integer such that \( 1 + N_v \cdot a_v = \# \{ E(k(v)) \} \), the number of rational points of the reduction of \( E \) to \( k(v) \).

For the remaining non-archimedean primes, \( L_v \) can be given explicitly as a polynomial in \( N_v^{-s} \) and for the archimedean prime, \( L_v = (2\pi)^{-s} \Gamma(s)^2 \), where \( \Gamma(s) \) is the classical \( \Gamma \)-function.

One defines the (classical) \( L \)-function \( L(E, \chi, s) \) to be the product of all the Euler factors \( L_v \) (including \( v = \infty \)). It is easily seen to be convergent to an analytic function in a suitable right half-plane. By Rankin's method (cf. [26]), one knows that \( L(E, \chi, s) \) extends to an entire function satisfying the functional equation:

\[
L(E, \chi, 2 - s) = e \cdot A^{s-1} \cdot L(E, \chi^{-1}, s)
\]

for \( e = e(E, \chi) \in C \) and \( A = A(E, \chi) \), suitable constants.

Let us distinguish two cases:

**The Exceptional Case.** \( E/\mathbb{Q} \) has complex multiplication by the field \( k \).

**The Generic Case.** Either \( E/\mathbb{Q} \) has no complex multiplication, or its field of complex multiplication is different from \( k \).

In the exceptional case, the \( L \) function \( L(E, \chi, s) \) factors into a product of two \( L \) functions attached to Grossencharacters over \( k \). Specifically,

\[
L(E, \chi, s) = L(\Phi, \chi, s) \cdot L(\Phi\varepsilon, \chi, s),
\]

where \( \Phi \) is the Grossencharacter attached to \( E/\mathbb{Q} \) and \( \varepsilon \) is the quadratic character belonging to \( k \). Moreover, one has the functional equation:

\[
L(\Phi, \chi, 2 - s) = e \cdot A^{s-1} L(\Phi, \chi^{-1}, s)
\]

for suitable constants \( e = e(\Phi, \chi), A = A(\Phi, \chi) \).

For anti-cyclotomic characters, the functional equation simplifies to read:

\[
L(E, \chi, 2 - s) = e \cdot A^{s-1} \cdot L(E, \chi, s)
\]

and

\[
L(\Phi, \chi, 2 - s) = e \cdot A^{s-1} \cdot L(\Phi, \chi, s) \quad \text{(in the exceptional case)},
\]

where, in either case, the constant \( e \) is \( \pm 1 \).

**6. Signs.** If \( \chi \) is anti-cyclotomic, define the sign of \( (E, \chi) \) to be \( e(\varphi, \chi) \) in the exceptional case and \( e(E, \chi) \) in the generic case. Thus the sign of \( (E, \chi) \) determines the parity of the order of vanishing of \( L(E, \chi, s) \) at
The problem of calculating \( \text{sign}(\ell, \chi) \) has been studied extensively. From a representation-theoretic point of view, we have Jacquet's [26], Chapter V, which draws on the techniques of [27]. See also Weil's [65]. From a slightly different point of view, see Kurcanov [32]. For calculations germane to our setting, see Gross [20] for the generic case and for the exceptional case, Greenberg [17]. For the interesting question of signs of elliptic curves over \( \mathbb{Q} \), see Kramer and Tunnell [33].

For later purposes we content ourselves with two formulas valid in the generic case:

(a) Let \( N \) be prime to the discriminant of \( k \). Let \( \chi_0 \) be the principal Hecke character over \( k \), and \( s \) the quadratic Dirichlet character attached to \( k \). Then \( \text{sign}(\ell, \chi_0) = -s(N) \) (e.g., if the pair \((k, \ell)\) satisfies the Heegner hypothesis of Section 5, then \( \text{sign}(\ell, \chi_0) = -1 \)).

(b) If \( \chi \) is an anti-cyclotomic character of conductor prime to \( N \), then \( \text{sign}(\ell, \chi) = \chi(N) \cdot \text{sign}(\ell, \chi_0) \).

7. Analytic rank versus arithmetic rank. Let \( q(\ell, \chi) \) denote the order of vanishing of \( L(\ell, \chi, s) \) at \( s = 1 \) (the "analytic rank"). Viewing \( \chi \) as a Galois character via class field theory, we have the "arithmetic rank" \( \rho(\ell, \chi) \) defined as in Section 2.

The conjectures of Birch and Swinnerton-Dyer (weakened and strengthened a bit) lead one to

**The Rank Conjecture:** \( q(\ell, \chi) = \rho(\ell, \chi) \).

8. The theory of Gross-Zagier. Gross and Zagier [22], [23] establish a magnificent formula which is, as they describe it, a new kind of Kronecker limit formula. A version of (special cases of) this formula had been previously conjectured by Birch [4], [5] and Stephens with significant numerical evidence compiled in its support. We shall describe, below, a slightly weakened version of the Gross-Zagier theorem.

Let

\[
f(z) dz = \sum_{n \geq 1} a_n e^{2\pi i n z} dz
\]

(with \( a_1 \) equal to 1 and not \( 2\pi i \)) be the new form on \( \Gamma_0(N) \) associated to \( \ell \), in the sense that there is a holomorphic differential \( \omega \) on \( E \), such that \( \varphi^* \omega = f(z) dz \).

Let \( \chi \) be an anti-cyclotomic character on \( k \), primitive on \( H \). Suppose that \( c \) is relatively prime to \( N \), and the Heegner hypothesis holds for \((0, N)\).
Then the Heegner hypothesis also holds for \((\mathcal{O}_c, \mathcal{N})\). Let \(w(\chi, \mathcal{N})\) be the Heegner point in \(V(E, \chi)\), the \(\chi\)-part of the Mordell–Weil group as in § 2. Let

\[
\|w(\chi, \mathcal{N})\|^2 = \langle w(\chi, \mathcal{N}), w(\chi, \mathcal{N}) \rangle
\]

be the square of the norm of \(w(\chi, \mathcal{N})\) in the Hermitian structure of \(V(E, \chi)\) determined by the height pairing. This is independent of the choice of \(\mathcal{N}\).

Under our hypotheses, we are in the generic case and the sign of \((E, \chi)\) is \(-1\). Therefore \(L(E, \chi, 1)\) vanishes.

**Theorem** (Gross–Zagier). There is a positive constant \(C\) such that

\[
L'(E, \chi, 1) = C \cdot \|w(\chi, \mathcal{N})\|^2.\]

The reader is referred to the forthcoming papers of Gross and Zagier for a full account. One can read the formula in either direction, with important consequences ensuing. Notably, by finding Heegner points which vanish, Gross and Zagier manage to produce \(L\)-functions with high order of vanishing at \(s = 1\), which by the prior work of Goldfeld [13] then provides an effective solution to the problem of listing quadratic imaginary fields of class number \(\leq B\) for any bound \(B\).

But also, in the context in which their theorem applies, if \(L'(E, \chi, 1)\) doesn’t vanish, their formula shows that the Heegner point \(w(\chi, \mathcal{N})\) is nonzero and hence if \(q(E, \chi) = 1\), then \(r(E, \chi) \geq 1\).

Gross and Zagier prove their formula by first providing just the right (infinite sum) expression for each side of their formula. These expressions have the virtue that there is a one-to-one correspondence between terms on the left and on the right. To prove their formula, they must establish an equality between corresponding terms and then deal with the highly nontrivial convergence problems that stand in their way. The infinite sum expression on the left comes naturally from Rankin’s method for treating \(L(E, \chi, s)\). The infinite sum expression on the right comes from an expression for the archimedean contribution to the height in terms of Green’s functions as well as a finite sum coming from the nonarchimedean contributions.

9. Non vanishing of \(q(E, \chi)\): the theory of Waldspurger. The theory alluded to has a number of deep arithmetic consequences. See Waldspurger’s

---

\[
\text{Gross and Zagier give an expression for } C \text{ in terms of the Petersson inner product of } f \text{ with itself, and elementary invariants. They can also work with certain Shimura curve parametrizations in place of the Weil parametrization to obtain a formula for the canonical heights of “Heegner points” coming from these parametrizations as well.}\
\]
account of this theory in the proceedings of this Congress. One corollary of his work is:

**Theorem.** There is an infinity of odd quadratic Dirichlet characters \( \chi \) such that if \( k_\chi \) is the (quadratic imaginary) field associated to \( \chi \), then \( (k_\chi, N) \) satisfies the Heegner hypothesis and \( \varphi(E|\mathbb{Q}, \chi) = 0 \).

10. Evidence for the “rank conjecture”. By the fundamental work of Coates–Wiles [8], as refined by Karl Rubin [54], we know that if \( E \) has complex multiplication, then \( \varphi(E, \chi) = 0 \) implies that \( r(E, \chi) = 0 \).

The result of Gross and Zagier tells us that if \( E/\mathbb{Q} \) is an arbitrary (Weil parametrized) elliptic curve, the Heegner hypothesis is satisfied for \( (\mathfrak{c}, N) \), and \( \chi \) is an anti-cyclotomic character primitive on \( \mathcal{H}_c \), then, \( \varphi(E, \chi) = 1 \) implies that \( r(E, \chi) \geq 1 \). If we are in the “exceptional case”, the Heegner hypothesis is not met. But by choosing an auxiliary quadratic imaginary field, using results of Waldspurger § 9, [62], [63] one can show that \( \varphi(E, \chi) = 2 \) implies that \( r(E, \chi) \geq 2 \).

11. Galois-conjugate characters. If \( \chi: \text{Gal}(\bar{k}/k) \to \mathbb{C}^\ast \) is a character, let \( Q(\chi) \) denote the subfield of \( \mathbb{C} \) generated by its values. If \( r: Q(\chi) \to Q(\chi^r) \) is a field automorphism and \( \chi^r \) the composition of \( r \) with \( \chi \), we refer to \( \chi \) and \( \chi^r \) as Galois-conjugate characters. Since \( r(E, \chi) = r(E, \chi^r) \), the “rank conjecture” would imply that

**Conjecture.**

\[
\varphi(E, \chi) = \varphi(E, \chi^r)
\]

and for even this weaker conjecture we have only fragmentary evidence. Namely: By some results of Shimura, or by the theory of modular symbols, one knows that \( \varphi(E, \chi) \) vanishes if and only if \( \varphi(E, \chi^r) \) does.

It follows from the theorem of Gross and Zagier that if \( \chi \) is anti-cyclotomic, primitive on \( \mathcal{H}_c \), \( \mathfrak{c} \) is prime to \( N \) and the Heegner hypothesis holds for \( (\mathfrak{c}, N) \), then \( \varphi(E, \chi) = 1 \) if and only if \( \varphi(E, \chi^r) = 1 \), and in the exceptional case, \( \varphi(\mathfrak{D}, \chi) = 1 \) if and only if \( \varphi(\mathfrak{D}, \chi^r) = 1 \).

12. Vertical anti-cyclotomic variation and Greenberg’s theory. In his beautiful paper [17] (see also the subsequent reference [18]), Ralph Greenberg proved the first deep general theorems about the vertical anti-cyclotomic variation of Mordell–Weil rank. Greenberg works in the exceptional case,

\[\text{See also [21], [59].}\]

\[\text{Compare Conjecture 2.7 of [10].}\]
and to prove his theorems he initiated an elegant method which blends archimedean techniques (for estimating special values of \(L\) functions attached to Grossencharacters) with \(p\)-adic techniques (where Greenberg makes essential use of Yager's two-variable \(p\)-adic \(L\) functions for more than one prime \(p\) and of Perrin–Riou's descent-theoretic study of the \(p\)-Selmer group \([46]\)).

Subsequently, Rohrlich \([50]\) discovered another approach to the same vertical problem which has very surprising points of similarity and difference to Greenberg's theory. For example, the archimedean estimate proved by Greenberg is a certain Abel mean summability property for the special values \(L(\Phi^{2k+1}, \chi, k+1)\). Greenberg shows that under the appropriate condition of sign, the Abel sums taken over \(k\) in certain arithmetic progressions are nonzero. To do this, he makes use of the (archimedean) Roth's theorem. He then appeals to the theory of \(p\)-adic \(L\) functions, and deduces parts \(A\) of the theorem and corollary below as well as a weaker version of part \(B\) of the corollary \((r_p(E, \chi) \geq 2)\).

Rohrlich, on the other hand, establishes a different type of convergence. He makes no use of \(p\)-adic \(L\) functions, but does use the \((p\)-adic) version of Roth's theorem in his theory. Is there a way of unifying the two approaches?

13. Rohrlich’s theory of Galois-averages. Let us suppose that we are in the exceptional case, with Grossencharacter \(\Phi\). Fix a finite set of primes \(S\) of \(k\), and let \(X_S\) denote the set of anti-cyclotomic characters over \(k\) whose conductor has prime divisors belonging to \(S\). Then \(X_S = X_S^+ \sqcup X_S^-\), where \(X_S^\pm\) denotes the subset of characters \(\chi\) for which the sign of \((E, \chi)\) is \(\pm 1\). Let

\[
\mathcal{L}(\Phi, \{\chi\}) = 1/|\mathcal{O}(\chi) : \mathcal{O}| \cdot \sum_{\tau \in \text{Gal}(\mathcal{O}(\chi)/\mathcal{O})} L(\Phi, \chi^\tau, 1)
\]

be the average value of \(L(\Phi, \chi^\tau, 1)\) over the set of characters \(\chi^\tau\) which are Galois-conjugate to \(\chi\). Rohrlich's remarkable discovery is that the average values \(\mathcal{L}(\Phi, \{\chi\})\) tend to a nonzero limit as \(\chi^\tau\) ranges through an infinite set of characters in \(X_S^+\) such that \(f(\chi^\tau)\) divides \(f(\chi^\tau+1)\).

Letting

\[
\mathcal{L}'(\Phi, \{\chi\}) = 1/|\mathcal{O}(\chi) : \mathcal{O}| \cdot \sum_{\tau \in \text{Gal}(\mathcal{O}(\chi)/\mathcal{O})} L'(\Phi, \chi^\tau, 1)
\]

denote the average value of the first derivatives, Rohrlich shows that for any constant \(c \in \mathbb{R}\) there are only a finite number of \(\chi\) in \(X_S^-\) such that \(|\mathcal{L}'(\Phi, \{\chi\})| \leq c\).
Using known facts (as described in Section 11) concerning invariance of $\nu(E, \chi)$ under Galois conjugation of $\chi$, Rohrlich deduces:

**Theorem.** Suppose that we are in the exceptional case. Then for all but a finite number of characters $\chi$ in $X_S$,

$$\nu(E, \chi) = 0 \quad \text{if the sign of } (E, \chi) \text{ is } +1 \quad (A)$$

and

$$\nu(E, \chi) = 2 \quad \text{if the sign of } (E, \chi) \text{ is } -1. \quad (B)$$

Using known facts (as described in Section 10), he then obtains:

**Corollary.** Suppose that we are in the exceptional case. Then for all but a finite number of characters $\chi$ in $X_S$,

$$r(E, \chi) = 0 \quad \text{if the sign of } (E, \chi) \text{ is } +1 \quad (A)$$

and

$$r(E, \chi) > 2 \quad \text{if the sign of } (E, \chi) \text{ is } -1. \quad (B)$$

Briefly, the technique of Rohrlich's proof is to express the Dirichlet series $L(\Phi, \chi, 1)$ as a sum of two types of terms: those terms that are visibly invariant under Galois-conjugation of $\chi$ (the "fixed" part) and those that "vary" (the "varying part"). The fixed part can be expressed as a nonzero multiple of $L(s, 1)$, that multiple being constant for large enough $f(\chi_i)$. The varying part is shown to have Galois-average tending to zero, by an ingenious use of (the $p$-adic version of) Roth's theorem. His treatment of $L'(\Phi, \chi, 1)$ is similar.

In the light of some work of Asai [1], [2], it is tempting to conjecture that the format of Rohrlich's theory carries over in the generic case as well (although the techniques of proof may not).

Let

$$L(E, \{\chi\}) = 1/[O(\chi): Q] \cdot \sum_{\text{regal}(Q(x)/Q)} L(E, \chi, 1),$$

and

$$L'(E, \{\chi\}) = 1/[O(\chi): Q] \cdot \sum_{\text{regal}(Q(x)/Q)} L'(E, \chi, 1).$$

**Conjecture.** Suppose that we are in the generic case.

Let $\chi_i$ be a sequence of characters in $X_S^+$ such that $f(\chi_i)$ divides $f(\chi_{i+1})$. 
Then
\[ \mathcal{L}(E, \{\chi_i\}) \text{ tends to a nonzero limit.} \]

Let \( \chi_i \) be an infinite sequence of characters in \( X_S \). Then
\[ |\mathcal{L}'(E, \{\chi_i\})| \text{ tends to infinity.} \]

A consequence of this conjecture together with Rohrlich's theorem is the following:

**Conjecture.** For all but a finite number of characters in \( X_S \) we have

\[ e(E, \chi) = 0 \quad \text{if the sign of } (E, \chi) \text{ is } +1, \]

\[ e(E, \chi) = 1 \quad \text{if the sign of } (E, \chi) \text{ is } -1, \]

\[ \text{and we are in the generic case,} \]

\[ e(E, \chi) = 2 \quad \text{if the sign of } (E, \chi) \text{ is } -1, \]

\[ \text{and we are in the exceptional case.} \]

14. Cyclotomic vertical variation. If \( E/Q \) is a Weil parametrized elliptic curve, \( S \) a finite set of primes of \( Q \) and \( Y_S \) = the set of Dirichlet characters (over \( Q \)) whose conductors have prime divisors belonging to \( S \), is it true that there are no more than a finite number of characters \( \chi \in Y_S \) such that \( e(E, \chi) \neq 0 \)?

Rohrlich has recently proved this to be true under the hypothesis that no prime in \( S \) divides \( N \), the conductor of \( E \). He adapts his method of Galois-averages to obtain this result. Using it, together with the work of Rubin [54] complementing that of Coates–Wiles [8], he obtains

**Theorem.** Let \( E/Q \) be an elliptic curve of complex multiplication and conductor equal to \( N \). Let \( F \) be an (infinite) abelian extension of \( Q \) unramified at \( \infty \) and outside a finite set of primes \( S \), none of which divide \( N \). Then \( E(F) \) is finitely generated.

The above theorem would also be true for arbitrary Weil curves \( E/Q \) if, for example, the rank conjecture (§7) were true. The reader is also referred to the papers [55] and [56], where Rubin and Wiles prove something close to the above theorem by first showing certain \( \text{mod } p \) congruences between special values of \( L \) functions and Bernoulli numbers, and then invoking the deep result of Washington [64] and their extension by Friedman [12] to show that the Bernoulli numbers in question are rarely congruent to zero \( \text{mod } p \). For a general discussion on congruences, see Stevens [61].
15. $Z_p$-extensions and $p$-adic logarithms over $k$. If $K$ is a numberfield and $A^*_K/K^*$ its idele class group, then any nontrivial continuous homomorphism from $A^*_K/K^*$ to $R^+$, the additive group of reals, must factor through the idele norm mapping $A^*_K/K^*\to R^*/(\pm 1)$. Consequently, to give such a homomorphism is equivalent to giving a "logarithm mapping", i.e., an isomorphism $R^*/(\pm 1)\cong R^+$.

Define a $p$-adic logarithmic character over $K$ (or a $p$-adic logarithm over $K$ for short) to be any continuous homomorphism

$$\lambda: A^*_K/K^*\to Q_p^+.$$  

The space of $p$-adic logarithms over $K$ forms a finite-dimensional $Q_p$-vector space of dimension $\geq r_2+1$, where $r_2$ is the number of complex archimedean places of $K$. A conjecture of Leopoldt asserts that its dimension is precisely $r_2+1$; this is known to be true for fields $K$ which are abelian over $Q$, by the work of Brumer.

In the case where $K = Q$, the space of $p$-adic logarithms is one-dimensional, with a natural choice of generator $\sigma$ determined by the prescription that $\sigma$ restricted to $Q_p^*\hookrightarrow A^*_K$ be $\log_p$, the standard $p$-adic logarithm. We refer to $\sigma$ as the $p$-cycloetomnic logarithm over $Q$; for $K$ any number field, the $p$-cycloetomnic logarithm over $K$ is the composition of $\sigma$ with the norm mapping $A^*_K/K^*\to A^*_Q/Q^*$.

By Class field theory, any $p$-adic logarithm $\lambda$ over $K$ determines (and is determined by) a unique continuous homomorphism

$$\lambda_{Gal}: \text{Gal}(\overline{K}/K)\to Q_p^+.$$  

If $\lambda$ is nontrivial, then the image of $\lambda_{Gal}$ is $p^N\cdot Z_p$ for some integer $N$, and so the kernel of $\lambda_{Gal}$ has, as fixed field, a $Z_p$-extension $L|K$, i.e., a Galois extension such that $\text{Gal}(L/K)$ is isomorphic to the additive group $Z_p$. We refer to $L|K$ as the $Z_p$-extension of $K$ cut out by $\lambda$. The space of $Z_p$-extensions of $K$ are then in one-to-one correspondence with the $Q_p$-projective space of lines through the origin in the vector space of $p$-adic logarithms over $K$.

If $k$ is a quadratic imaginary number field, by an anti-cycloetomnic $p$-adic logarithm we mean a nontrivial logarithm over $k$ whose $k/Q$ conjugate is equal to its negative. Choose such an anti-cycloetomnic logarithm $\tau$. Then any $p$-adic logarithm of $k$ is a $Q_p$-linear combination of $\sigma$ and $\tau$.

The theory of $Z_p$-extensions was initiated by Iwasawa as a suitable framework for the study of asymptotic questions concerning the rate of growth of $(p$-primary components of) ideal class groups. For the arithmetic of elliptic curves, as John Coates once remarked, $Z_p$-extensions serve
as an invaluable tool: they provide an amenable setting for the study of the \( p \)-adic vertical variation problem (e.g., as described in Section 2), a setting which is congenial to the method of \( p \)-power descent. Moreover, via their associated \( p \)-adic logarithms, \( \mathbb{Z}_p \)-extensions give rise to a theory of \( p \)-adic heights (for \( p \) ordinary) and to a theory of \( p \)-adic \( L \) functions which, conjecturally, should mesh very well with the arithmetic theory and provide a manageable computational handle on it.

16. The pro-\( p \)-Selmer group. If one is to make use of \( p \)-power descent theory to study the Mordell–Weil group, it is natural to work with the \( \mathbb{Z}_p \)-module
\[
\mathcal{E}(K)_p = [\mathcal{E}(K)/\text{torsion}] \otimes \mathbb{Z}_p
\]
rather than with \( \mathcal{E}(K) \) itself. However, even this \( \mathbb{Z}_p \)-module is only indirectly approachable by descent-theoretic methods; for example, with our present state of knowledge, it would be difficult to prove any regularity of the growth of the \( \mathbb{Z}_p \)-rank of \( \mathcal{E}(K_n)_p \) as \( K_n \) runs through the \( n \)-th layers of a \( \mathbb{Z}_p \)-extension \( L/K \).

It has been traditional to replace \( \mathcal{E}(K)_p \) by the pro-\( p \)-Selmer group \( \text{Sel} \mathcal{E}_p(E/K) \) for which such “growth regularity” theorems can be proved, and which is conjecturally (via the Shafarevich–Tate conjecture) equal to \( \mathcal{E}(K)_p \). We sketch the definition of the pro-\( p \)-Selmer group.

Let \( K \) be any number field, \( E \) an elliptic curve over \( K \) and \( p \) a prime number. Recall the classical \( p \)-Selmer group, defined to make the square
\[
\begin{array}{ccc}
\text{Sel} \mathcal{E}_p(E/K) & \to & H^2(\text{Gal}(\overline{K}/K), E[p^\infty]) \\
\downarrow \, i & & \downarrow \, j \\
\bigwedge H^1(\text{Gal}(\overline{K}/K_\infty), E[p^\infty]) & \to & H^1(\text{Gal}(\overline{K}/K), E[p^\infty])
\end{array}
\]
cartesian, where \( i \) and \( j \) are the natural morphisms, and \([p^\infty]\) means the union of the kernels of multiplication by \( p^n \) for all \( n \geq 0 \). The Shafarevich–Tate group of \( E \) over \( K \) is denoted \( \bigwedge H^1(E/K) \). It is defined to be the intersection of the kernels
\[
H^1(\text{Gal}(\overline{K}/K), E) \to H^1(\text{Gal}(\overline{K}/K_v), E),
\]
where \( v \) runs through all places (archimedean and nonarchimedean) of \( K \). There is a natural mapping
\[
\mathcal{E}(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \text{Sel} \mathcal{E}_p(E/K)
\]
which is injective, and induces an injection on Tate modules. Note that
\[
\mathcal{E}(K)_p = T_p(\mathcal{E}(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p) = \text{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, \mathcal{E}(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p).
\]
Let $S_p(E, K)$ stand for
\[ T_p(S\text{elmer}_p(E/K)) = \text{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, \text{Selmer}_p(E/K)). \]
The Shafarevitch–Tate conjecture implies that

**CONJECTURE.** The natural injection
\[ E(K)_p \hookrightarrow S_p(E/K) \]
is an equality.

If $r_p(E, K)$ denotes the $\mathbb{Z}_p$-rank of $S_p(E/K)$, we have the inequality
\[ r(E, K) \leq r_p(E, K) \]
(conjecturally an equality).

### 17. $Z_p$-extensions and universal norms

Let $K$ be a number field $L/K$, an infinite Galois extension with Galois group $T$ isomorphic to $\mathbb{Z}_p$. Let $K_n$ be the "$n$-th layer" of the extension $L/K$ with Galois group $T_n$ isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. Denote by $A$ the Iwasawa ring
\[ \mathbb{Z}_p[[T]] = \lim_{\rightarrow} \mathbb{Z}_p[T_n]. \]

By a system of $T_n$-modules, $A_n(n \geq 0)$ is meant a sequence of such modules together with inclusions
\[ i: A_j \rightarrow A_k, \quad j \leq k \]
and "norm" mappings
\[ N_{k, j} = N: A_k \rightarrow A_j, \quad k \geq j \]
compatible with $T$-module structures such that the composition $iN: A_k \rightarrow A_k$ is given by the natural norm mapping\(^9\) (from $T_k$ to $T_j$).

Given such a system, define the **subsystem of a universal norms** by the rule
\[ UA_j = \bigcap_{k \geq j} N_{k, j} A_k \subseteq A_j. \]

The natural injections $i: A_j \rightarrow A_k$ preserve the submodules of universal norms, as do the mappings $N$.

---

\(^9\) There is, perhaps, greater justification in referring to this as a *trace* rather than a norm, but our prototype is class field theory where $A$ is the multiplicative group of a field.
If the $A_j$ are $\mathbb{Z}_p$-modules of finite type, then the norm mappings 

$$N: UA_k \to UA_j$$

are surjective. Let $UA$ stand for the projective limit of the $UA_k$ compiled via the norm mappings above, and viewed as a $A$-module.

18. Growth numbers. Using the theory of $A$-modules and [36], Prop. 6.4, one can show:

**Growth Number Proposition.** Suppose that $E$ has good ordinary reduction at every place $v$ of $K$ of characteristic $p$. Suppose further that for any $v$ such that the Néron model of $E$ at $v$ is geometrically disconnected, $v$ splits only finitely often in $L$.

Then there is an integer $a$ (independent of $n$) such that the $L/K$ universal norm submodule $US_p(E, K_n) \subset S_p(E, K_n)$ is a free $A_n$-module of rank $a$, for all $n$.

We have the following asymptotic behavior for the ranks:

$$r_p(E, K_n) = a \cdot p^n + e_n$$

where the "error terms" $e_n$ are nonnegative numbers monotonically increasing with $n$ and admitting a uniform upper bound.

We refer to the integer $a = a(E, L/K)$ as the growth number of $E$ for the $\mathbb{Z}_p$-extension $L/K$.

Let us return to $K = k$ a quadratic imaginary field and $E/\mathbb{Q}$ a Weil parametrized elliptic curve. Compatible with the conjectures and results quoted in Section 2, we have the

**Growth Number Conjecture.** Let $p$ be a prime number of good, ordinary reduction for $E$. Suppose that the Néron fibre of $E$ is geometrically connected at every place $v$ of $k$ at which the $\mathbb{Z}_p$-extension $L/k$ splits infinitely. Then:

$$a(E, L/k) = 0$$

if $L/k$ is not the anti-cyclotomic $\mathbb{Z}_p$-extension, or the sign of $(E, \chi_0)$ is $+1$. (Here $\chi_0$ is the principal character over $k$.)

If $L/k$ is the anti-cyclotomic $\mathbb{Z}_p$-extension and the sign of $(E, \chi_0)$ is $-1$, then:

$$a(E, L/k) = 1$$

in the generic case,

and:

$$a(E, L/k) = 2$$

in the exceptional case.
Remarks. (1) A more general growth number proposition could be proved concerning $\chi$-eigenspaces for $\chi$ a tame character (i.e., of finite order prime to $p$) over $k$. We content ourselves here and in Sections 19, 20 and 22 below with statements for $\chi = \chi_0$, the principal character, although more general tame characters could also be treated.

(2) See Monsky [41]–[43] for an analysis of possible growth behavior in $Z_p[[Z_p^d]]$ modules for general $d \geq 1$.

19. Heegner points as universal norms. Let $k \subseteq \mathcal{O}$ be a quadratic imaginary field, $p$ a prime number, and $N$ a positive integer prime to $p$, for which there exists an ideal $\mathcal{N}$ in the ring of integers $\mathcal{O}$ of $k$, of norm $N$. Fix such an ideal $\mathcal{N}$. Let $\mathfrak{o}_n$ denote the order in $\mathcal{O}$ of conductor $p^n$, and $\mathcal{N}_n = \mathcal{N} \cap \mathfrak{o}_n$. Let $H_n$ be the ring class field of $\mathfrak{o}_n$, so that $H_n = k(j(\mathfrak{o}_n))$. If $H_\infty = \bigcup H_n$, then $H_\infty$ is an anti-cyclotomic extension of $k$ whose Galois group is isomorphic to $Z_p \oplus F$ where $F$ is a finite group; consequently, there is a unique $Z_p$-extension $K_\infty/k$ contained in $H_\infty$. The $Z_p$-extension $K_\infty/k$ is the anti-cyclotomic $Z_p$-extension of $k$.

Define

$$K_n = K_\infty \cap H_n \quad \text{for all } n \geq 0.$$ 

Thus $K_\emptyset/k$ is a finite, cyclic, everywhere unramified extension of degree a power of $p$, and $K_n/K_\emptyset$ is a finite cyclic extension totally ramified at the primes dividing $p$, and of degree $p^n$.

Let $\varphi : X_0(N) \to \mathcal{E}$ be a Weil parametrization of an elliptic curve $\mathcal{E}/\mathbb{Q}$ (of conductor $N$).
Define the submodule of Heegner points at the $n$-th layer
\[ \mathcal{E}(K_n) = \text{Trace}_{H_n/K_n} \{ \sigma(\mathcal{O}_n, \mathcal{N}_n) \}, \quad \sigma \in \text{Gal}(H_n/K), \]
to be the $\mathbb{Z}_p$-module generated by the trace to $K_n$ of the basic Heegner points of level $p^n$. Thus, if
\[ e_n^\sigma = \text{Trace}_{H_n/K_n} \{ \sigma(\mathcal{O}_n, \mathcal{N}_n) \}, \quad e_n^\sigma \in \mathbb{Z}_p, \]
then $\mathcal{E}(K_n)$ is the $\mathbb{Z}_p$-module generated by the $e_n^\sigma$ (for $\sigma \in \text{Gal}(H_n/K)$) in $\mathbb{E}(K_n) \otimes \mathbb{Z}_p / \text{torsion}$.

Now let $a_p$ denote the integer $1 + p - \#(E(F_p))$, and let $\beta_p, \bar{\beta}_p$ denote the two roots of $X^2 - a_p X + p$. Suppose that $p$ is ordinary for $E$, i.e., $a_p \not\equiv 0 \mod p$, and that $\beta_p$ is the $p$-adic unit root.

Let $\epsilon$ denote the quadratic character belonging to $k$, so that $1 + \epsilon(p)$ is the number of distinct primes of $k$ with residue field $F_p$. Let $M_p = \beta_p - 1 - \bar{\epsilon}(p)$. Then $M_p$ is never zero.

Using formulas expressing the action of the Hecke operator $T_p$ on Heegner points, an elementary calculation yields:

**Proposition.** Suppose that $a_p$ is congruent to neither 0 nor $1 + \epsilon(p)$ mod $p$. Then working in the system of $\mathbb{Z}$-modules $\mathbb{E}(K_n) \otimes \mathbb{Z}_p / \text{torsion}$, we have
\[ \text{Norm}_{K_m/K_n} \mathcal{E}(K_m) = \mathcal{E}(K_n), \quad m \geq n > 0. \]

More generally, if $a_p \not\equiv 0 \mod p$, then $M_p \mathcal{E}(K_n)$ lies in the subspace of $K_\infty/K_n$-universal norms.

For simplicity we suppose, now, that $a_p \not\equiv 0$, or $1 + \epsilon(p) \mod p$. Define the Heegner module
\[ \mathcal{E}(K_\infty) = \lim_{\rightarrow n} \mathcal{E}(K_n) \]
which is the analogue for our elliptic curve $E$ of the $\Lambda$-module constructed by taking the projective limit of the $p$-completion of the space of elliptic units in $K_n$, the limit being taken as $n$ tends to $\infty$.

One easily sees that the $\Lambda$-module $\mathcal{E}(K_\infty)$ is cyclic, and since the natural mapping $\mathcal{E}(K_\infty) \rightarrow US_p(K_\infty)$ is nontrivial if $\mathcal{E}(K_\infty) \not\equiv \{0\}$, and the latter $\Lambda$-module is free, it follows that $\mathcal{E}(K_\infty)$ is a free $\Lambda$-module of rank either 0 or 1. Clearly, if there exists some $n \geq 0$ for which $e_n$ is nonzero, then $\mathcal{E}(K_\infty)$ is free of rank 1.

**Conjecture.** There is some $n$ for which $e_n$ is nonzero; equivalently: $\mathcal{E}(K_\infty)$ is a free $\Lambda$-module of rank 1.
Remarks. (1) The theory we have just described can be generalized with some modification to eigenspaces for some character $\chi$ of order prime to $p$. As suggested in Section 4, one should broaden the theory to include Heegner points coming from the various Shimura curve parametrizations of $E$ as well.

(2) Kurcanov was the first to discover the possibility that Heegner points account for unbounded Mordell-Weil rank in anti-cyclotomic towers. See [32] for examples of nontriviality of Heegner modules attached to certain tame characters $\chi$.

(3) It is worth noting that although the $A$-module structure of $E(K_\infty)$ is simple enough, the structure of the finite layers $E(K_n)$ can be quite subtle and, invoking standard conjectures, can be seen to reflect properties of the error term $e_n$ in the formula

$$r_p(E, K_n) = a \cdot [K_n : k] + e_n.$$  

20. $p$-adic heights. The classical height pairing on the Mordell–Weil group of an elliptic curve involves the choice of an $\mathbb{R}$-valued logarithmic character $\lambda : \mathbb{A}_K^* \rightarrow \mathbb{R}$

although the use of the “natural logarithm” obscures this choice.

A general “theory of $p$-adic heights” for elliptic curves $E/K$ would yield a bilinear symmetric pairing

$$E(K) \times E(K) \rightarrow \mathbb{Q}_p,$$

$$\langle x, y \rangle \rightarrow \langle x, y \rangle_\lambda$$

dependent upon a choice of $p$-adic valued logarithm $\lambda$ over $K$ (a canonical $\lambda$-height pairing) which is $\mathbb{Q}_p$-linear in $\lambda$, functorial, and, of course, satisfies the more elusive property of being an effective tool in the study of the arithmetic of $E$.

We do not yet have such a general theory, but much progress towards it has been recently made.

Say that a logarithm $\lambda$ over $K$ is ordinary for $E$ if for every nonarchimedean prime $v$ of $K$ at which $\lambda$ is ramified, either the Néron fibre of $E$ is of multiplicative type or the “Trace of Frobenius” $\alpha_v$ is not congruent to zero modulo the characteristic of the residue field of $v$. Say that $\lambda$ is good for $E$ if for every $v$ at which $\lambda$ is ramified, $E$ has good reduction.

Suggestions for a mod-$p$ theory first appeared in [53]. For elliptic curves of complex multiplication and for certain ordinary $p$-adic logarithms,
Perrin-Riou [47] and Bernardi [3] developed an analytic theory. Perrin-Riou also produced an arithmetic (i.e., "descent-theoretic") definition in the same context and she established the equivalence of the two theories. More recently, Schneider [57] has given a general formulation of the theory of arithmetic height, valid for general elliptic curves $E$ and good\(^{10}\) ordinary logarithms for $E$. He also discovered another way of defining the height under the same hypothesis and has shown that his two definitions are equivalent. We refer to this as Schneider's $p$-adic height. Néron has yet another approach [44]. Gross and Oesterlé have a $p$-adic height for complex multiplication elliptic curves and good non-ordinary logarithms for $E$. In [38], a theory of $p$-adic heights for general elliptic curves and ordinary logarithms is developed; we refer to this as analytic $p$-adic height.

The Schneider $\lambda$-height pairing has the desirable property that its kernel contains the subspace of $L/K$-universal norms, where $L/K$ is the $\mathbb{Z}_p$-extension cut out by the logarithm $\lambda$. The analytic height pairing, being "analytic", is amenable to numerical calculation. One can prove that Schneider's theory coincides with the analytic theory for good, ordinary, logarithms, but see the forthcoming [39] for a surprise in a more general context.

Now choose a basis $P_1, \ldots, P_r$ for the Mordell-Weil group $E(K)$ modulo torsion. Consider

$$\delta(\lambda) = \det_q \langle P_i, P_j \rangle_\lambda,$$

viewed as giving rise to an $r$-linear symmetric form (the height determinant form) on the space of $p$-adic logarithms over $k$ which are ordinary for $E$.

It would follow from the conjecture of Section 16 and the above discussion that if $\delta(\lambda) \neq 0$, i.e., the $\lambda$-height pairing is nondegenerate, then the growth number of $L/K$, the $\mathbb{Z}_p$-extension cut out by $\lambda$, vanishes.

What $r$-linear forms can arise as height determinant forms? See forthcoming work of G. Brattström related to this question.

21. The ($p$-adic valued) analytic theory. If $\chi$ is a Hecke character of finite order over $k$, let $Q(\chi) \subset \mathbb{C}$ denote the subfield generated by the values of $\chi$. By the recent work of Cogdell–Stevens [9], there is a nonzero complex number $\Omega_E$ (the period) such that the special values

$$\Lambda(E, \chi) \overset{\text{def.}}{=} L(E, \chi, 1)/\Omega_E$$

lie in the field $Q(\chi)$.

\(^{10}\) Schneider's theory also covers certain cases of bad ordinary reduction.
Now let \( A \) be any integer, \( p \) a prime of good, ordinary reduction for \( E \) and \( G_{p, A} \) the Galois group of the union of all abelian extensions of \( k \) of conductor dividing \( p^m \cdot A \) for some \( m \). From the work of Kurcanov, following that of Manin (See also Haran [24]), one sees that there is a \( Q_p \)-valued measure \( \mu_{p, A} \) on \( G_{p, A} \) (i.e., a distribution with bounded values) which "\( p \)-adically interpolates" the special values \( \Lambda(E, \chi) \) in the sense that we have a formula of the form:

\[
\int \chi \cdot \mu_{p, A} = c_{p, A}(E, \chi) \cdot \Lambda(E, \chi)
\]

valid in \( Q(\chi) \otimes Q_p \), where \( \chi \) is any character of \( k \) of conductor dividing \( p^m \cdot A \) for some \( m \) (viewed on the left-hand side as a character on \( G_{p, A} \)), and where \( c_{p, A}(E, \chi) \) is a nonzero "elementary term"; elementary in the sense that its dependence on \( E \) is purely local: it can be expressed in terms of the Euler factors \( L_v \) of \( E \) for \( v \) dividing \( pA \).

For a fixed character \( \chi \) of conductor equal to \( A \) as above, and a \( p \)-adic logarithm \( \lambda \), we may define the \( p \)-adic \( L \) function (in the \( \lambda \) direction) as the power series in \( Q(\chi) \otimes Q_p[[X]] \):

\[
L_\lambda(\chi; X) = \sum_{n=0}^{\infty} \frac{1}{n!} \int \lambda^n \cdot \chi \cdot \mu_{p, A} \cdot X^n
\]

and, making use of our choice of cyclotomic and anti-cyclotomic \( p \)-adic logarithms \( \sigma \) and \( \tau \), we define the two-variable \( p \)-adic \( L \) function by:

\[
L_{\sigma, \tau}(\chi; S, T) = \sum_{n, m \geq 0} \frac{1}{n! \cdot m!} \int \chi \cdot \sigma^n \cdot \tau^m \cdot \mu_{p, A} \cdot S^n T^m.
\]

Clearly, the substitution \( S = aX, T = bX \) in the two-variable \( p \)-adic \( L \) series yields the \( p \)-adic \( L \) series in the \( \lambda = a\sigma + b\tau \) direction.

The results on \( p \)-adic interpolation are obtained by working with modular symbols attached to lifts of the automorphic form determined by the Weil parametrized elliptic curve \( E \).

There has been an impressive output of work devoted to the establishment of a one-variable theory of \( p \)-adic \( L \)-functions (principally in the cyclotomic direction but see [6], [7] for very interesting results in different directions). As for the two-variable theory, prior to the work of Kurcanov and Haran, Katz [29], [30] and Manin–Visik [35] defined a \( p \)-adic \( L \) function attached to Grossencharacters over a quadratic imaginary field, by interpolation of special values of certain Eisenstein series.
and Yager [66], [68], [69] provided an alternative approach to Katz's $L$-functions by considering the images of elliptic units in local units.

If $v$ denotes $k|Q$-conjugation, since one can show that

$$
\tau_A = \tau_p A,
$$

we have:

$$
L_{\omega, \tau}(\chi; S, T) = L_{\omega, \tau}(\chi; S, -T).
$$

We also have the functional equation for characters $\chi$ of conductor $\ell$ prime to $N$ which can be written

$$
L_{\omega, \tau}(\chi; S, T) = e(E, \chi) \cdot \exp \left( S \cdot \sigma(N) \right) \cdot \chi(N) \cdot L_{\omega, \tau}(\chi^{-1}; -S, -T)
$$

for a suitable constant $e(E, \chi)$. Combining the above two equations when $\chi$ is anti-cyclotomic gives:

$$
L_{\omega, \tau}(\chi; S, T) = e(E, \chi) \cdot \exp \left( S \cdot \sigma(N) \right) \cdot L_{\omega, \tau}(\chi; -S, T)
$$

again under the hypothesis that $\ell$ is prime to $N$. The constant $e(E, \chi)$ is the sign of $(E, \chi)$ in the generic case.

From the functional equation one readily sees that when the sign of $(E, \chi)$ is $-1$ ($\chi$ anti-cyclotomic, $\ell$ prime to $N$), the anti-cyclotomic $L$ series $L_{\tau}(\chi; X)$ vanishes identically. In this case, define the first derived anti-cyclotomic $L$ series by the formula:

$$
L'_{\omega, \tau}(\chi; X) \overset{\text{def.}}{=} \partial / \partial S \{ L_{\omega, \tau}(S, X) \} |_{S=0}.
$$

In the exceptional case, when the sign is $-1$, the first derived anti-cyclotomic $L$ series will also vanish and it is the second derived $L$ series which will be of interest.

Concerning the two-variable $p$-adic $L$ function, it would be very interesting to frame precise conjectures connecting it to the arithmetic of $Y$ along the lines that have been explored in analogy with conjectures already formulated in the one-variable theory.

Notably, one might hope for a "main conjecture" which relates the locus of zeros of $L_{\omega, \tau}$ in a suitable ball to the divisorial part of the support of an Iwasawa module built from $p$-primary Selmer groups. One might hope for a "Birch–Swinnerton–Dyer-type conjecture" which would assert that if the two-variable $p$-adic $L$ series is written as an infinite sum

$$
\sum_{j \geq 0} \psi_j^{(\omega, \tau)}(\chi; S, T)
$$

where $\psi_j^{(\omega, \tau)}(\chi; S, T)$ is a homogeneous polynomial of degree $j$ in the variables $S$ and $T$ and $\psi_0^{(\omega, \tau)}(\chi; S, T)$ is the lowest nonvanishing term, then $\nu = r(E, \chi)$ and $\nu$ is a scalar multiple of a suitable "height determinant form" (cf.
Section 20). One might hope to pin down that scalar multiple. One would expect a "theory of congruences modulo Eisenstein primes" along the lines of the one-variable theory [37], [61].

22. $p$-adic valued Heegner measures. Let us return to the setting of Section 19. Choose a generator $c_\infty$ of the Heegner module $\mathcal{S}(K_\infty)$. Let $c_n \in \mathcal{S}(K_n)$ be the image of $c_\infty$. Define a $Q_p$-valued measure $\nu_n$ on $\Gamma_n$ by the rule:

$$\nu_n(g) = p^n \langle c_n, c_n^g \rangle,$$

where $\langle \cdot, \cdot \rangle$ denotes the $p$-adic valued height attached to $c$, the $p$-cyclo-
tomic logarithm.

One easily checks that the $(\nu_n)_n$ satisfy the distribution law

$$\nu_n(g) = \sum_{g'} \nu_{n+1}(g')$$

where the sumation runs through all elements of $\Gamma_{n+1}$ projecting to $g$ in $\Gamma_n$. Thus the $(\nu_n)_n$ determine a distribution $\nu$ on $\Gamma$, which can be seen (using the results of [38]), to be a measure, i.e., $\nu^{(c_\infty)} \in \Lambda \otimes_{\mathbb{Z}_p} Q_p$. Changing the choice of generator $c_\infty$ of $(K_\infty)$ changes $\nu^{(c_\infty)}$ by multiplication by a unit in $\Lambda$.

Is there a $p$-adic version of the theory of Gross and Zagier, which relates the first derived $p$-anti-cyclotomic $L$-function $L'_*(\chi_0, X)$ to the Heegner measure $\nu^{(c_\infty)}$?

References


Modular Curves and Arithmetic

[53] Rosenblum M. in collaboration with Abramov S., The Birch Swinnerton-Dyer Conjecture mod $p$, handwritten manuscript.


