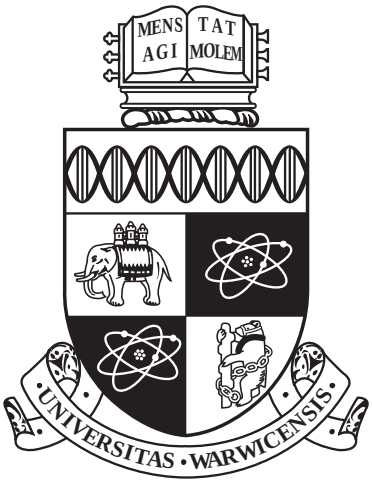

Elliptic Curves with Complex Multiplication; The Coates–Wiles Theorem

by

Daniel Lewis

Thesis

Submitted to The University of Warwick

Mathematics Institute

April, 2013

THE UNIVERSITY OF
WARWICK

Contents

1 Complex Multiplication

1.1 Basic theory

Elliptic curves are curves of genus 1 with a specified basepoint, denoted ∞. More specifically, if K is a field with $\text{char}(K) \neq 2, 3$, then an elliptic curve E over K is given by a *short Weierstrass equation* of the form

$$E : y^2 = x^3 + ax + b$$

where $a, b \in K$, and *discriminant* $\Delta = -(4a^3 + 27b^2) \neq 0$. The *j-invariant* of E is

$$j(E) = -1728\frac{4A^3}{\Delta}.$$

Definition 1.1. Let $P, Q \in E(\overline{K})$. We define the addition law $\oplus$ on $E(\overline{K})$ as follows: we first draw the line L through P and Q (if $P \neq Q$) or the tangent line (if $P = Q$), and let $P * Q$ be its third intersection point with $E(\overline{K})$. Then we draw the line through $P * Q$ and ∞, and let $P \oplus Q$ be its third intersection point with $E(\overline{K})$. In symbols,

$$P \oplus Q = (P * Q) * \infty.$$

Fact 1.2. Let E be an elliptic curve defined over a field K. Then $E(\overline{K})$ is an additive abelian group under the operation $\oplus$, with identity element ∞.

Definition 1.3. Let E_1 and E_2 be elliptic curves. An *isogeny* between E_1 and E_2 is a morphism

$$\phi : E_1 \to E_2$$

satisying $\phi(\infty) = \infty$. We say E_1 and E_2 are *isogenous* if there is an isogeny $\phi : E_1 \to E_2$ with $\phi(E_1) \neq \{\infty\}$.

Since elliptic curves are groups, isogenies between them form groups. Let

$$\text{Hom}(E_1, E_2) = \{\text{isogenies } \phi : E_1 \to E_2\}.$$

Then 1.2 implies that $\text{Hom}(E_1, E_2)$ is a group under the addition law

$$(\phi + \psi)(P) = \phi(P) \oplus \psi(P).$$

If $E_1 = E_2$ then we can also compose isogenies.

Definition 1.4. If E is an elliptic curve, we define the *endomorphism ring* of E,

$$\text{End}(E) = \text{Hom}_{\overline{K}}(E, E),$$

to be the ring with addition as above and multiplication given by composition:

$$(\phi\psi)(P) = \phi(\psi(P)).$$

Example 1.5. For each $m \in \mathbb{Z}$ we can define the *multiplication by m* isogeny

$$[m] : E \to E$$

as follows:
if $m > 0$ then

$$[m](P) = \underbrace{P \oplus P \oplus \cdots \oplus P}_{m \text{ terms}};$$

if $m < 0$ then $[m](P) = [-m](-P)$; and $[0](P) = \infty$.

Example 1.6. Let E be an elliptic curve over a finite field $\mathbb{F}_q$, where $q = p^n$ and $p \in \mathbb{Z}$ is prime. We have a *Frobenius endomorphism*

$$\begin{aligned} \phi_q : E(\overline{\mathbb{F}_q}) &\to E(\overline{\mathbb{F}_q}) \\ (x, y) &\mapsto (x^q, y^q). \end{aligned}$$

The following proposition will prove useful later in this section.
Proposition 1.7. *Let E be an elliptic curve over $\mathbb{F}_q$. Then we have*

$$\#E(\mathbb{F}_q) = \#\ker(1 - \phi_q) = \deg(1 - \phi_q).$$

Proof. We shall only prove the first equality, the second requires the idea of *separable* endomorphisms[1], which is sadly one diversion too many.
Let $P = (x, y) \in E(\overline{F}_q)$; we see that

$$\begin{aligned} P \in E(\mathbb{F}_q) \iff (x^q, y^q) = (x, y) &\iff \phi_q(P) = P \\ &\iff (1 - \phi_q)(P) = 0 \iff P \in \ker(1 = \phi_q). \end{aligned}$$

So $E(\mathbb{F}_q) = \ker(1 - \phi_q)$. □

Fact 1.8. The Frobenius endomorphism satisfies the characteristic polynomial

$$F(x) = x^2 - a_q x + q,$$

where $a_q = q + 1 - \#E(\mathbb{F}_q)$ (is the *trace of Frobenius*).

Proof. See Silverman [Si 1, V §2]. □

[1] For details, see Lassina Dembélé's course notes on Elliptic Curves, or Silverman [Si 1, §2]

Remark 1.9. Suppose that $\mathrm{char}(K) = 0$. Then the map

$$[\ ] : \mathbb{Z} \to \mathrm{End}(E)$$

is in most cases an isomorphism.

Definition 1.10. If $\mathrm{End}(E) \ncong \mathbb{Z}$, then we say that E has *complex multiplication.*

Remark 1.11. If K is a finite field, then E always has complex multiplication. (Consider the Frobenius endomorphism.)

1.2 Examples

It may be illustrative to see a few examples of elliptic curves over $\mathbb{C}$ with complex multiplication, to demonstrate that such curves do indeed exist.

Example 1.12. Let $E/\mathbb{C}$ be the elliptic curve

$$E : y^2 = x^3 - x.$$

Then $\mathrm{End}(E)$ contains (in addition to $\mathbb{Z}$) an element $[i]$ given by

$$[i] : (x, y) \mapsto (-x, iy).$$

Thus E has complex multiplication. Now

$$[i] \circ [i] : (x, y) \mapsto (-(-x), i^2 y) = (x, -y) = [-1](x, y),$$

so $[i] \circ [i] = [-1]$, and so we have a ring homomorphism

$$\begin{aligned} \mathbb{Z}[i] &\to \mathrm{End}(E) \\ m + ni &\mapsto [m] + [n] \circ [i]. \end{aligned}$$

In fact, this is an isomorphism. So E has complex multiplication by $\mathbb{Z}[i]$.

1.3 Two notable results

Elliptic curves with complex multiplication possess many special and rather interesting properties. To delve headlong into this theory would take several pages, and lead us too far astray of our goal: the Coates–Wiles Theorem. Therefore, I will only state two of the main theorems. The interested reader should consult Silverman [Si 2], an invaluable resource.

First, we must recall an important definition from Class Field Theory:

Definition 1.13. The *Hilbert class field* of K, denoted H, is the maximal abelian extension of K that is unramified at all primes.

With this in mind, we may now state the first of the two aforementioned theorems.

Theorem 1.14. *Let $K/\mathbb{Q}$ be a quadratic imaginary field with ring of integers $\mathcal{O}_K$, and let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$. Then $K(j(E))$ is the Hilbert class field H of K.*

Proof. See Silverman [Si 2, II §4]. □

This is a quite remarkable and unexpected result, as is the next theorem, which does not require any further definitions to comprehend.

Theorem 1.15. *Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication. Then $j(E)$ is an algebraic integer.*

Proof. See Silverman[2] [Si 2, II §6]. □

This last theorem is best illustrated by a concrete example. To ease calculation, let us choose a quadratic imaginary field of class number 1.

Example 1.16. Consider the field $K = \mathbb{Q}(\sqrt{-43})$ and its ring of integers $\mathcal{O}_K = \mathbb{Z}[\alpha]$, where $\alpha = \frac{1+\sqrt{-43}}{2}$. It is routine to check that $\mathcal{O}_K$ has class number 1. It therefore follows that $j(\mathcal{O}_K) \in \mathbb{Z}$. Recall from the theory of modular forms that $j(z)$ has q-expansion

$$j(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots,$$

where $q = e^{2\pi iz}$. If we substitute $z = \alpha$, then

$$q = e^{i\pi(1+\sqrt{-43})} = -e^{-\pi\sqrt{43}} = -1.13027972081179 \times 10^{-9} \approx -1.130 \times 10^{-9}$$

is small, so the dominant term in the q-expansion is $1/q$, which should be close to integral. Calculation shows $1/q = -884736743.999775 \approx -884736744$, and so

$$j(E) = 884735999.999775 \approx -884736000 = -960^3 = -2^{18}3^35^3.$$

This provides a numerical verification of Theorem 1.15 for this example.

1.4 The Grössencharacter

Elliptic curves with complex multiplication possess an associated Grössencharacter. In order to explain what a Grössencharacter is, we first introduce the idele group.

Let K be a number field, and for each absolute value v of F, let K_v be the completion of K at v. Also, let $\mathcal{O}_v$ be the ring of integers of K_v if v is non-archimedean, and let $\mathcal{O}_v = K_v$ otherwise.

[2] Silverman in fact produces three separate proofs. The Complex Analytic proof is perhaps the easiest to follow.

Definition 1.17. The *idele group* of K is the group

$$\mathbb{A}_K^* = \prod_v{}' K_v^*,$$

where the dash signifies that the product is restricted relative to the $\mathcal{O}_v$'s. That is, an element $x \in \prod K_v^*$ is in $\mathbb{A}$ if and only if $s_v \in \mathcal{O}_v^*$ for all but finitely many v.

If L/K is a finite extension of number field, then there is a natural *norm* map from $\mathbb{A}_L^*$ to $\mathbb{A}_K^*$. This is the continuous homomorphism

$$\mathrm{N}_K^L : \mathbb{A}_L^* \to \mathbb{A}_K^*$$

defined by sending $x \in \mathbb{A}_L^*$ to the element of $\mathbb{A}_K^*$ with v-th component

$$\prod_{w|v} \mathrm{N}_{K_v}^{L_w} x_w.$$

Definition 1.18. A *Grössencharacter* on a number field L is a continuous homomorphism

$$\psi : \mathbb{A}_L^* \to \mathbb{C}^*$$

satisying $\psi(L^*) = 1$.

Definition 1.19. Let $\mathfrak{P}$ be a prime of a number field L. A Grössencharacter $\psi : \mathbb{A}_L^* \to \mathbb{C}^*$ is *unramified* at $\mathfrak{P}$ if $\psi(\mathcal{O}_{\mathfrak{P}}^*) = 1$.

Now it is clear what a Grössencharacter is, it remains to describe such a map. The calculations are unavoidably long-winded, see Silverman [Si 2, II §9] for full details. The following theorem provides a summary of his results:

Theorem 1.20. *Suppose L/K is a finite extension of number fields, and let E/L be an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$ of K. Let $x \in \mathbb{A}_L^*$ be an idele of L, and let $s = \mathrm{N}_K^L x \in \mathbb{A}_K^*$. Then there exists a unique $\alpha = \alpha_{E/L}(x) \in K^*$ with the following two properties:*

(i) $\alpha\mathcal{O}_K = (s)$, where $(s) \subset K$ is the ideal of s.

(ii) For any fractional ideal $\mathfrak{a} \subset K$ and any analytic map

$$f : \mathbb{C}/\mathfrak{a} \to E(\mathbb{C}/\mathfrak{a}),$$

the following diagram commutes

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\alpha s^{-1}} & K/\mathfrak{a} \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\ E(L^{\mathrm{ab}}) & \xrightarrow{[x,L]} & E(L^{\mathrm{ab}}). \end{array}$$

Remark 1.21. (i) It is rather striking that (s) is principal; a priori this certainly need not be the case.

(ii) Again, it is quite remarkable that f maps K to $E(L^{\mathrm{ab}})$. That statement alone could be a theorem in its own right.

Theorem 1.22. *Again suppose L/K is a finite extension of number fields, and let E/L be an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$ of K.*
For any idele $s \in \boldsymbol{A}_K^*$, let $s_\infty \in \mathbb{C}^*$ be the component of s corresponding to the unique archimidean absolute value on K. If we define a map

$$\begin{aligned} \psi_{E/L} : \mathbb{A}_L^* &\to \mathbb{C}^* \\ x &\mapsto \alpha_{E/L}(x)\, \mathrm{N}_K^L(x^{-1})_\infty, \end{aligned}$$

then

1. *$\psi_{E/L}$ is a Grössencharacter of L.*
2. *Let $\mathfrak{P}$ be a prime of L. Then $\psi_{E/L}$ is unramified at $\mathfrak{P}$ if and only if E has good reduction at $\mathfrak{P}$.*

Proof. See Silverman [Si 2, II, Theorems 9.1 and 9.2]. □

This Grössencharacter will be very useful to us in Chapter 3. But now, let us consider another important and closely related tool at our disposal: the *L-series* attached to an elliptic curve with complex multiplication.

1.5 L-Series

The L-series is an analytic function that encodes additional arithmetic information about the elliptic curve. The reader may be aware that modular forms possess analogous L-series[3]; in this subsection I will define the analogous L-function for an elliptic curve with complex multiplication.

Let $L/\mathbb{Q}$ be a number field, and let E/L be an elliptic curve. For each prime $\mathfrak{P}$ of L, let

$$\begin{aligned} \mathbb{F}_{\mathfrak{P}} &= \text{ residue field of } L \text{ at } \mathfrak{P}, \\ q_{\mathfrak{P}} &= \mathrm{N}_{\mathbb{Q}}^L \mathfrak{P} = \#\mathbb{F}_{\mathfrak{P}}. \end{aligned}$$

Definition 1.23. 1. If E has good reduction at $\mathfrak{P}$, we first define

$$a_{\mathfrak{P}} = q_{\mathfrak{P}} + 1 - \#\tilde{E}(F_{\mathfrak{P}}).$$

[3] If $f = \sum_{n=1}^\infty a_n q^n \in S_k(\Gamma_1(N))$, then $L(f,s) = \sum_{n=1}^\infty a_n n^{-s}$ is well-defined and holomorphic in s, for $\Re(s) > 1 + k/2$.

Then the *local L-series of E at $\mathfrak{P}$* is the polynomial $L_{\mathfrak{P}}(E/L,T)$ defined by

$$L_{\mathfrak{P}}(E/L,T) = 1 - a_{\mathfrak{P}}T + q_{\mathfrak{P}}T^2.$$

2. If E has bad reduction at $\mathfrak{P}$, we define the local L-series according to the following three cases

$$L_{\mathfrak{P}}(E/L,T) = \begin{cases} 1-T & \text{if } E \text{ has split multiplicative reduction at } \mathfrak{P}, \\ 1+T & \text{if } E \text{ has non-split multiplicative reduction at } \mathfrak{P}, \\ 1 & \text{if } E \text{ has additive reduction at } \mathfrak{P}. \end{cases}$$

Piecing together these local L-factors, we can form the global L-series of E:

Definition 1.24. The *(global) L-series of E/L* is defined by the Euler product

$$L(E/L,s) = \prod_{\mathfrak{P}} L_{\mathfrak{P}}(E/L, q_{\mathfrak{P}}^{-s})^{-1},$$

where the product is over all primes of L.

Notice that neither of the above definitions require the elliptic curve E/L to have complex multiplication. If E does have complex multiplication, recall from the previous subsection that E has an attached Grössencharacter, that is, a continuous homomorphism $\psi : \mathbb{A}_L^* \to C^*$ which satisfies $\psi(L^*) = 1$.

Let $\mathfrak{P}$ be a prime of L at which ψ is unramified, so $\psi(\mathcal{O}_{\mathfrak{P}}) = 1$. Then we define

$$\psi(\mathfrak{P}) = \psi(\dots, 1, 1, \underbrace{\pi}_{\mathfrak{P}\text{-th component}}, 1, 1, \dots),$$

where π is a uniformizer[4] at $\mathfrak{P}$. Since ψ is unramified at $\mathfrak{P}$, $\psi(\mathfrak{P})$ is well-defined, independent of the choice of π.

For ψ ramified at $\mathfrak{P}$, set $\psi(\mathfrak{P}) = 0$.

Definition 1.25. The *Hecke L-series attached to the Grössencharacter $\psi : \mathbb{A}_L^* \to \mathbb{C}^*$* is defined by the Euler product

$$L(s,\psi) = \prod_{\mathfrak{P}} (1 - \psi(\mathfrak{P}) q_{\mathfrak{P}}^{-s})^{-1},$$

where the product is over all primes of L.

Hecke's Theorem states that Hecke L-series have analytic continuation to the entire complex plane; moreover, there is a functional equation relating its values at s and $N-s$, for some $N = N(\psi) \in \mathbb{R}$. This is a powerful statement, and all the more so combined with

[4] Defined in Silverman [Si 1, II §1].

the following result:

Theorem 1.26 (Deuring)**.** *Let E/L be an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$ of K.*

1. *Suppose that $K \subset L$. Let $\psi_{E/L} : \mathbb{A}_L^* \to \mathbb{C}^*$ be the Grössencharacter attached to E/L. Then*
$$L(E/L, s) = L(s, \psi_{E/L})L(s, \overline{\psi_{E/L}}).$$

2. *Suppose that $K \not\subset L$, and let $L' = LK$. Further let $\psi_{E/L'} : \mathbb{A}_{L'}^* \to \mathbb{C}^*$ be the Grössencharacter attached to E/L'. Then*
$$L(E/L, s) = L(s, \psi_{E/L'}).$$

It follows that the L-series of an elliptic curve with complex multiplication has an analytic continuation to the entire complex plane, and satisfies a functional equation relating its values at s and $2 - s$.

1.6 A worked example

At this point it seems appropriate to include a concrete example to illustrate the theory of Grössencharacters and L-functions that we have covered in the previous subsections. Silverman provided the following example in the form of two exercises [Si 2, exercises 2.33, 2.34].

Example 1.27. Let $D \in \mathbb{Z}$ be a non-zero integer, and let E be the elliptic curve
$$E : y^2 = x^3 - Dx,$$
with complex multiplication by the ring of integers $\mathcal{O}_K = \mathbb{Z}[i]$ of the field $K = \mathbb{Q}(i)$. Let $p \in \mathbb{Z}$ be a prime with $p \nmid 2D$.

Claim 1. If $p \equiv 3 \pmod 4$, then
$$\#\tilde{E}(\mathbb{F}_p) = p + 1 \quad \text{and} \quad \#\tilde{E}(\mathbb{F}_{p^2}) = (p+1)^2.$$

Proof. Consider the map
$$\begin{aligned} \psi : \mathbb{F}_p &\to \mathbb{F}_p \\ x &\mapsto x^3 - Dx. \end{aligned}$$
It is easy to see that $\psi(-x) = -\psi(x)$ (i.e. ψ is odd). For $x \neq 0$, this means that
$$\psi(x) \text{ is a square} \iff \psi(-x) \text{ is a non-square.}$$

So, by quadratic reciprocity, there are $\frac{p-1}{2}$ values of x_0 for which $\psi(x_0)$ is a square. Each such value yields 2 points $(x_0, \pm y_0) \in \tilde{E}(\mathbb{F}_p)$, with $y_0^2 = \psi(x_0)$. The points $(0,0)$ and ∞ are also in $\tilde{E}(\mathbb{F}_p)$. Hence

$$\#\tilde{E}(\mathbb{F}_p) = 2\left(\frac{p-1}{2}\right) + 1 + 1 = p + 1.$$

Thus, referring back to Fact 1.8, the trace of Frobenius $a_p = 0$, and so $(\phi_p)^2 + p = 0$. Notice that $(\phi_p)^2 = \phi_{p^2}$ (immediate from the definition), so $(\phi_{p^2} + p)^2 = 0$ and the trace $a_{p^2} = -2p$. So we have

$$\#\tilde{E}(\mathbb{F}_{p^2}) = p^2 + 1 - a_{p^2} = (p+1)^2.$$

□

If $p \equiv 1 \pmod 4$, we may factor p in $\mathbb{Z}[i]$ as

$$p = \pi\bar{\pi} \quad \text{with } \pi \equiv 1 \pmod{2+2i}.$$

Claim 2. In this case,

$$\#\tilde{E}(\mathbb{F}_p) = p + 1 - \overline{\left(\frac{D}{\pi}\right)_4}\,\pi - \left(\frac{D}{\pi}\right)_4 \bar{\pi}, \tag{1.1}$$

where $\left(\frac{\alpha}{\pi}\right)_4$ is the 4^{th}-power residue symbol; that is, $\left(\frac{\alpha}{\pi}\right)_4$ is the 4^{th}-root of unity satisfying $\alpha^{(\mathrm{N}_{\mathbb{Q}}^K \mathfrak{p}-1)/4} \equiv \left(\frac{\alpha}{\pi}\right)_4 \pmod{\pi}$.

Proof. See Ireland-Rosen [I–R, Ch. 18, §4]. □

Now let $\mathfrak{p} \subset \mathbb{Z}[i]$ be a prime ideal with $\mathfrak{p} \nmid 2D$. Write

$$\mathfrak{p} = (\pi) \text{ for an element } \pi \in \mathbb{Z}[i] \text{ satisying } \pi \equiv 1 \pmod{2+2i}.$$

Claim 3. The Grössencharacter associated to $E/\mathbb{Q}(i)$ is given explicitly by the formula

$$\psi_{E/\mathbb{Q}(i)}(\mathfrak{p}) = \overline{\left(\frac{D}{\pi}\right)_4}\,\pi.$$

Here $\psi_{E/\mathbb{Q}(i)}(\mathfrak{p})$ equals the value of ψ at an idele with a uniformizer at the $\mathfrak{p}^{\text{th}}$ component and 1's elsewhere.

Proof. Using equation 1.1 together with Silverman's Corollary 10.4.1 [Si 2, p.175], we see

that the Grössencharacter associated to $E/\mathbb{Q}(i)$ is given either by

$$\psi_{E/\mathbb{Q}(i)}(\mathfrak{p}) = \overline{\left(\frac{D}{\pi}\right)_4}\,\pi \quad \text{or else by} \quad \psi_{E/\mathbb{Q}(i)}(\mathfrak{p}) = \left(\frac{D}{\pi}\right)_4\,\overline{\pi}.$$

To determine which one it is, we use Silverman's Corollary 5.4 [Si 2, p.133] to find a root of unity $\xi \in \mathbb{Z}[i]^*$ such that the reduction of $[\xi\pi]$ modulo $\mathfrak{p}$ is $N_{\mathbb{Q}}^{\mathbb{Q}(i)}\mathfrak{p}$-power Frobenius. (This is possible for almost all degree 1 primes of $\mathbb{Q}(i)$). On the other hand, Silverman's Proposition 10.4 [Si 2, p.174] says that $[\psi_{E/\mathbb{Q}(i)}(\mathfrak{p})]$ also reduces to Frobenius. Thus we can conclude that

$$\psi_{E/K}(\mathfrak{p}) = \overline{\left(\frac{D}{\pi}\right)_4}\,\pi, \qquad \text{where } \mathfrak{p} = (\pi) \text{ and } \pi \equiv 1 \pmod{2+2i},$$

at least for almost all degree 1 primes $\mathfrak{p}$ of $\mathbb{Q}(i)$. By the continuity of ψ and the reciprocity law for $\left(\frac{\cdot}{\pi}\right)_4$, we see that this formula holds for almost all $\mathfrak{p}$. □

We can now (using Theorem 1.26 and the fact that $N_{\mathbb{Q}}^{\mathbb{Q}(i)}$) write down the L-series of E over $\mathbb{Q}(i)$ and over $\mathbb{Q}$ explicitly using residue symbols as

$$L(E/\mathbb{Q}(i), s) = \prod_{\substack{\pi \in \mathbb{Z}[i] \text{ prime} \\ \pi \equiv 1 \pmod{2+2i}}} \left(1 - \overline{\left(\frac{D}{\pi}\right)_4}\,\pi^{1-s}\bar{\pi}^{-s}\right)^{-1} \times \left(1 - \left(\frac{D}{\pi}\right)_4\,\pi^{-s}\bar{\pi}^{1-s}\right)^{-1},$$

$$L(E/\mathbb{Q}, s) = \prod_{\substack{\pi \in \mathbb{Z}[i] \text{ prime} \\ \pi \equiv 1 \pmod{2+2i}}} \left(1 - \overline{\left(\frac{D}{\pi}\right)_4}\,\pi^{1-s}\bar{\pi}^{-s}\right)^{-1}$$

2 Galois Cohomology

In this section we introduce group cohomology and present the key theoretical results needed for our assault on the Coates–Wiles Theorem. Some familiarity with Algebraic Topology may clarify these results, but is certainly not a prerequisite.

2.1 Group Cohomology

Let G be a group.

Definition 2.1. A *G-module* is an abelian group A together with an action of G; that is, there is a homomorphism $\phi : G \to \mathrm{Aut}(A)$. Usually we take $g \in G, a \in A$ and define $\phi(g)a = g \cdot a$ with the properties

$$g(a_1 + a_2) = ga_1 + ga_2,$$
$$g(g'a) = (gg')(a).$$

We can extend this to an action of $\mathbb{Z}[G]$ on A.

Definition 2.2. Given a G-module A as above, the subgroup of fixed elements of A (*G-invariants*) is

$$A^G = \{a \in A : ga = a \quad \forall g \in G\}.$$

We say that G *acts trivially on* A if $ga = a$ for all $g \in G, a \in A$; thus $A^G = A$ if and only if the action is trivial.

We now define the cohomology groups $H^i(G, A)$ for $i \in \mathbb{N}$. Let

$$C^i(G, A) = \mathrm{Maps}(G^i, A),$$

with $G^0 = \{1\}$, so $C^0(G, A) = A$. An element of $C^i(G, A)$ is a function f of i variables in G, $f(g_1, \ldots, g_i) \in A$, and is called an *$i$-cochain*. Now, there is a sequence

$$0 \xrightarrow{0} C^0(G, A) \xrightarrow{\partial_0} C^1(G, A) \xrightarrow{\partial_1} C^2(G, A) \xrightarrow{\partial_2} \cdots$$

where the *coboundary maps* $\partial_i : C_i(G, A) \to C_{i+1}(G, A)$ are defined as follows. Give $C^i(G, A)$ a group structure pointwise and write $(g\phi)(x_1, \ldots, x_i) = g(\phi(x_1, \ldots, x_n))$. Set $\partial_{-1} = 0$. For $n \in \mathbb{N}$, let $f \in C^n(G, A),\ g_i \in G$. Then

$$\begin{aligned}\partial_n(f)(g_1, \ldots, g_{n+1}) = {} & g_1 f(g_2, \ldots, g_{n+1}) \\ & + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \ldots, g_{n+1}) \\ & + (-1)^{n+1} f(g_1, \ldots, g_n).\end{aligned}$$

This definition is quite complicated, so it helps to illustrate the first few cases:

$$\begin{aligned}\partial_0(f(g_1)) &= g_1 f - f \\ \partial_1(f(g_1,g_2)) &= g_1 f(g_2) - f(g_1 g_2) + f(g_1) \\ \partial_2(f(g_1,g_2,g_3)) &= g_1 f(g_2,g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1,g_2).\end{aligned}$$

Claim 4. $\partial_{i-1} \circ \partial_i = 0 \quad \forall i \in \mathbb{N}$.

Proof. This is an easy yet somewhat longwinded exercise. □

Definition 2.3. Let $n \in \mathbb{N}$.
If $z \in Z^n(G,A) = \ker \partial_n$, we call z an *n-cocycle.*
If $b \in B^n(G,A) = \operatorname{Im} \partial_{n-1}$, we call b an *n-coboundary.*
We then define the n^{th} *cohomology group*

$$H^n(G,A) = \frac{Z^n(G,A)}{B^n(G,A)}.$$

Example 2.4. Let G be a group, A a G-module. In the case $n = 0$, we have

$$\begin{aligned}B^0(G,A) &= \{0\}, \\ Z^0(G,A) &= \{f \in C^0(G,A) : gf = f \quad \forall g \in G\} = A^G,\end{aligned}$$

and hence $H^0(G,A) = A^G$.

In the case $n = 1$, we have

$$\begin{aligned}B^1(G,A) &= \{f : f(g) = ga - a \quad \text{for some } a \in A\}, \\ Z^1(G,A) &= \{f : f(g_1 g_2) = g_1 f(g_2) + f(g_1)\},\end{aligned}$$

and $H^1(G,A) = Z^1(G,A)/B^1(G,A)$.
Note that if G acts trivially, then $H^1(G,A) = \operatorname{Hom}(G,A)$.
Definition 2.5. Let G be a group, A a G-module. Given cochains $f \in C^k(G,A)$, $g \in C^l(G,A)$, we define their *cup product* $f \cup g \in C^{k+l}(G,A)$ by

$$(f \cup g)(\sigma) = f(\sigma|[v_0,\ldots,v_k]) \cdot g(\sigma|[v_{k+1},\ldots,v_{k+l}]).$$

We have [5]

$$\partial_{k+l}(f \cup g) = (\partial_k f) \cup g + (-1)^k (f \cup \partial_l g).$$

Thus $f \cup g$ is a cocycle if both f and g are cocycles; $f \cup g$ is a coboundary if one of the

[5] For proof, see Neukirch–Schmidt–Wingberg, Proposition 1.4.1 [NSW pp. 35, 36].

cochains f and g is a coboundary and the other a cocycle. So we have a well-defined map

$$H^k(X,A) \times H^l(X,A) \to H^{k+l}(X,A)$$
$$([f],[g]) \mapsto [f \cup g].$$

Definition 2.6. A *topological group* G is a group and topological space, such that the multiplication law $G \times G \to G$ and the inverse map $G \to G$ are continuous (with respect to the topology on G).

Definition 2.7. A *profinite group* is a topological group obtained as the inverse limit of a collection of finite groups, each equipped with the discrete topology.

Now suppose (for the remainder of this subsection) that G is profinite. The following two theorems, due to John Tate, will prove useful.

Theorem 2.8. *Suppose $i \geq 0$ and $T = \varprojlim_n T_n$, where each T_n is a finite (discrete) G-module. If $H^{i-1}(G, T_n)$ is finite for all n, then*

$$H^i(G,T) = \varprojlim_n H^i(G,T_n).$$

Theorem 2.9. *If T is a finitely generated $\mathbb{Z}_p$-module, then for every $i \geq 0$, $H^i(G,T)$ has no divisible elements, and*

$$H^i(G,T) \otimes \mathbb{Q}_p \xrightarrow{\sim} H^i(G, T \otimes \mathbb{Q}_p).$$

2.1.1 Inflation and Restriction

A morphism of pairs $(G,A) \to (G',A')$ is a map $G' \to G$ and a G'-homomorphism $A \to A'$, where G' acts on A via $G' \to G$. In particular, we may take G' to be a subgroup $H \leq G$. Two important examples of the above map are

- The *restriction* map
$$\mathrm{res} : H^r(G,A) \to H^r(H,A);$$
- The *inflation map*: For $H \trianglelefteq G$, with natural quotient map $G \to G/H$ and $A^H \subseteq A$, we have a map
$$\mathrm{inf} : H^r(G/H, A^H) \to H^r(G,A).$$

Fact 2.10. If H is a normal subgroup of G, then there is an exact sequence

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\mathrm{inf}} H^1(G,A) \xrightarrow{\mathrm{res}} H^1(H,A)^{G/H} \xrightarrow{d} H^2(G/H, A^H) \xrightarrow{\mathrm{inf}} H^2(G,A).$$

This is known as the *inflation-restriction sequence*, and the map d is called *transgression*.

2.2 Galois Cohomology

Now that we have the basic setup, we can introduce a few results in Galois Cohomology.

Definition 2.11. Let $E/\mathbb{Q}$ be an elliptic curve, and $l \in \mathbb{Z}$ a prime. Multiplication by l on the l-power torsion groups of E gives maps

$$E[l] \longleftarrow E[l^2] \longleftarrow E[l^3] \longleftarrow \cdots$$

The *(l-adic) Tate module of E* is the group

$$T_l(E) = \varprojlim_n E[l^n].$$

Tate modules of elliptic curves will prove to be invaluable tools in our later theory.

We now present Hilbert's[6] Theorem 90. Let L/K be a Galois extension, with profinite Galois group $G_{L/K} = \operatorname{Gal} L/K$. In general, we have

$$H^i(G, L^\times) \cong \varinjlim_{\substack{L \supset M \supset K \\ \text{finite, Galois}}} H^i(G_{M/K}, M^\times).$$

Theorem 2.12 (Hilbert's Theorem 90)**.** *We have $H^1(G_{L/K}, L^\times) = 1$.*

Let us proceed further; let μ_N be the group of N^{th} roots of unity (so $\mu_N \cong \mathbb{Z}/n\mathbb{Z}$). Then we have a short exact sequence

$$1 \longrightarrow \mu_N \longrightarrow \overline{K}^\times \xrightarrow{[N]} \overline{K}^\times \longrightarrow 1.$$

Thus we have a long exact sequence

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mu_N \cap K^\times & \longrightarrow & K^\times & \xrightarrow{[N]} & K^\times \\ & & & & & \overset{\delta}{\searrow} & \\ & & H^1(G_{\overline{K}/K}, \mu_N) & \longrightarrow & H^1(G_{\overline{K}/K}, \overline{K}^\times) & \longrightarrow & \cdots \end{array}$$

Since $H^1(G_{\overline{K}/K}, \overline{K}^\times) = 0$ (by Hilbert's Theorem 90), δ must be surjective. Hence we obtain

Theorem 2.13 (Kummer)**.** $H^1(G_{\overline{K}/K}, \mu_N) \cong K^\times/(K^\times)^N$.

[6] This is a misnomer; the theorem is actually due to Ernst Kummer, and was further generalised by Emmy Noether. David Hilbert presented it as Theorem 90 in his Zahlbericht, and the name has stuck.

Definition 2.14. Let $p \in \mathbb{Z}$ be prime, then we define $\mathbb{Z}_p(1) = \varprojlim_n \mu_{p^n}$.

By Kummer's Theorem, we have

$$\varprojlim_n H^1(G_{\overline{K}/K}, \mu_{p^n}) \cong \varprojlim_n K^\times/(K^\times)^{p^n}.$$

Since

$$H^0(G_{\overline{K}/K}, \mu_{p^n}) = \mu_{p^n} \cap K^\times < \infty \quad \forall n \in \mathbb{N},$$

by Tate's Theorem 2.8 we have

$$H^1(G_{\overline{K}/K}, \mathbb{Z}_p(1)) \cong K^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

Now let E be an elliptic curve over a number field K. We have a short exact sequence

$$0 \longrightarrow E[m] \longrightarrow E(\overline{K}) \xrightarrow{[m]} E(\overline{K}) \longrightarrow 0,$$

which gives us a long exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)[m] & \longrightarrow & E(K) & \xrightarrow{[m]} & E(K) \\ & & & & & \searrow^{\delta} & \\ & & H^1(G_{\overline{K}/K}, E[m]) & \longrightarrow & H^1(G_{\overline{K}/K}, E(\overline{K})) & \xrightarrow{[m]} & \cdots \end{array}$$

Thus we have a short exact sequence

$$0 \longrightarrow \tfrac{E(K)}{mE(K)} \xrightarrow{\delta} H^1(G_{\overline{K}/K}, E[m]) \longrightarrow H^1(G_{\overline{K}/K}, E(\overline{K}))[m] \longrightarrow 0,$$

and again by Tate's Theorem 2.8 we have

$$E(K) \otimes \mathbb{Z}_p = \varprojlim_n \frac{E(K)}{p^n E(K)} \xrightarrow{\delta} H^1(G_{\overline{K}/K}, T_p(E)).$$

2.2.1 Tate Duality

In this subsection we will consider cohomology of *local fields*, which are fundamental objects of study in number theory. A couple of preliminary definitions will be necessary:

Definition 2.15. A topological space X is *locally compact* if every point of X has a compact neighbourhood.

Definition 2.16. A *topological field* is a field K which is also a topological space, such that the addition and multiplication maps $K \times K \to K$ are continuous (with respect to the product topology), as is the inversion map $K^\times \times K^\times \to K^\times$.

Definition 2.17. A *local field* is a locally compact topological field with respect to a non-discrete topology.

We can define an absolute value on a local field, and the local field is then accordingly archimedean or non-archimedean.

Example 2.18.
- $\mathbb{R}$ and $\mathbb{C}$ are archimedean local fields (of characteristic zero).
- The p-adic numbers $\mathbb{Q}_p$ (where $p \in \mathbb{Z}$ is prime) are a non-archimedean local field of characterstic zero, as are finite extensions of $\mathbb{Q}_p$.

We will also need the following two definitions:

Definition 2.19. The *absolute Galois group* G_K of a field K is $\mathrm{Gal}(\overline{K}/K)$.

In the case that K is a non-archimedean local field, we write $G_K^{\mathrm{unr}} = \mathrm{Gal}\,(K_{\mathrm{unr}}/K)$.

Definition 2.20.
1. If G is a group (resp. profinite group), the *cohomological dimension* of G, denoted $\mathrm{cd}(G)$, is the least $n \in \mathbb{N}$ such that $H^i(G, A) = 0 \quad \forall i > n$, for all G-modules (resp. discrete G-modules) A.
2. For a prime p, we define the *cohomological p-dimension* of G, denoted $\mathrm{cd}_p(G)$, to be the least $n \in \mathbb{N}$ such that $H^i(G, A)(p) = 0 \quad \forall i > n$, for all G-modules A.

Theorem 2.21. *Let K be a non-archimedean local field of characteristic zero. Then*

1. *For any prime $p \in \mathbb{Z}$, we have $\mathrm{cd}_p(G_K) = 2$. Also, if L/K is of degree p^∞, then $\mathrm{cd}_p(G_L) \leq 1$.*
2. $$H^i(G_K, \mu_n) = \begin{cases} K^\times/(K^\times)^n & i = 1 \\ (\frac{1}{n}\mathbb{Z})/\mathbb{Z} & i = 2 \\ 0 & i \geq 3. \end{cases}$$
3. *If A is a finite G_K-module, then $H^i(G_K, A)$ is finite, for all $i \geq 0$.*

We are now almost ready to state Tate's Duality Theorem. Given a non-archimedean local field K, set $A^* = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$, and $A' = \mathrm{Hom}(A, \mu)$.

Theorem 2.22. *Let K be a finite field extension of $\mathbb{Q}_p$, and A a finite G_K-module. The cup product gives us a pairing*

$$H^i(K, A') \times H^{2-i}(K, A) \xrightarrow{\cup} H^2(K, \mu) \cong \mathbb{Q}/\mathbb{Z}, \tag{2.1}$$

which for $i \in \{0, 1, 2\}$ induces an isomorphism

$$H^i(K, A') \to H^{2-i}(K, A)^*.$$

We have a representation $\rho : G_K \to \mathrm{Aut}(A)$. We say that this representation is *unramified* if the inertia subgroup I of G_K is contained in $\ker(\rho)$. Equivalently, $A^I = A$. Notice that

$I \cong \mathrm{Gal}(\overline{K}, K_{\mathrm{unr}})$.

Definition 2.23. For a G_K-module A, we define the i^{th} *unramified cohomology group*

$$H^i_{\mathrm{unr}}(K, A) = \mathrm{Im}\left(H^i(G_K^{\mathrm{unr}}, A^I) \xrightarrow{\mathrm{inf}} H^i(G_K, A)\right).$$

Remark 2.24. $H^0_{\mathrm{unr}}(K, A) = H^0(K, A)$.

Theorem 2.25. *Let A be a finite unramified G_K-module, where K is a finite field extension of $\mathbb{Q}_p$. Then the groups $H^i_{unr}(K, A)$ and $H^{2-i}_{unr}(K, A)$ annihilate each other in the pairing (2.1). Moreover, they are mutually orthogonal complements.*

2.2.2 Euler–Poincaré characteristic

Let K be a non-archimedean local field of characteristic l, and let V be a finite-dimensional $\mathbb{Q}_p$ vector space. Set $h^i(K, V) = \dim H^i(K, V)$.

Definition 2.26. The *Euler–Poincaré characteristic* of V is given by

$$\chi(K, V) = \sum_i (-1)^i h^i(K, V) = h^0(K, V) - h^1(K, V) + h^2(K, V).$$

Thus

$$\chi(K, V) = \begin{cases} [K : \mathbb{Q}_p] \dim V & l = p, \\ 0 & l \neq p. \end{cases}$$

2.2.3 Cohomology of elliptic curves over finite fields

Let $E/\mathbb{F}_q$ be an elliptic curve. We define $V_l(E) = T_l(E) \otimes \mathbb{Q}_p$. Let us study the cohomology of $V_l(E)$.

The absolute Galois group $G_{\mathbb{F}_p}$ is topologically generated by the Frobenius endomorphism ϕ_p. Recall Fact 1.8: ϕ_p satisfies the characteristic polynomial $x^2 - a_p x + p$, where $a_p = p + 1 - \#E(\mathbb{F}_p)$. The *Hasse Inequality* states that $|a_p(E)| \leq 2\sqrt{p}$. This implies that 1 cannot be a solution of the characteristic polynomial. Thus

$$H^0(\mathbb{F}_p, V_l(E)) = V_l(E)^{\phi_p} = 0.$$

If A is a $\mathbb{Z}/mZ$ module, where $\mathbb{Z}/m\mathbb{Z} = \langle g \mid g^m \rangle$, then $H^1(\mathbb{Z}/m\mathbb{Z}, A) \cong \ker N/(g-1)A$, so

$$H^1(\mathbb{F}_p, V_l(E)) \cong \frac{\ker N}{(\phi_p - 1)V_l(E)} \cong V_l(E)/V_l(E) = 0,$$

and $H^i(\mathbb{F}_p, V_l(E)) = 0$ for every $i \geq 2$.

Now consider an elliptic curve E of good reduction over $\mathbb{Q}$. Since $H^i_{\mathrm{unr}}(G_{\mathbb{Q}_p}, V_l(E)) =$

$H^i(G_{\mathbb{Q}_p}^{\mathrm{unr}}, V_l(E)) = H^i(G_{\mathbb{F}_p}, V_l(E))$, we have

$$H^i_{\mathrm{unr}}(G_{\mathbb{Q}_p}, V_l(E)) = 0 \quad \text{for } i = 0, 1, 2.$$

It is quite a deep result that the converse is true as well (and, in fact, more is true):

Theorem 2.27 (Néron–Ogg–Shafarevich)**.** *For an elliptic curve $E/\mathbb{Q}_p$, the following are equivalent:*

1. *E has good reduction.*
2. *There is a prime $l \neq p$ such that the Tate module $T_l(E)$ is unramified.*
3. *$T_l(E)$ is unramified for all primes $l \neq p$.*

Proof. See Silverman [Si 1, VII §7]. □

2.2.4 The Poitou–Tate exact sequence

Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication. As before, define $V_p(E) = T_p(E) \otimes \mathbb{Q}_p$. The absolute Galois group $G_{\mathbb{Q}}$ acts on $V_p(E)$. Let S be a finite set of primes including p, ∞ and all primes dividing the discriminant Δ of E.

Fact 2.28. The action of $G_{\mathbb{Q}}$ (which we may think of as a "large" group, difficult to work with) factors through $G_{\mathbb{Q},s}$ (a more "reasonable" group, which is easier to work with).

Example 2.29. The group $H^1(G_{\mathbb{Q}}, \mathbb{F}_2) = \oplus_{\mathbb{N}} \mathbb{F}_2$ is countably infinite, whereas $H^1(G_{\mathbb{Q},s}, \mathbb{F}_2)$ is finite.

At a prime $l \in S$, there is a *localisation* map

$$H^i(G_{\mathbb{Q},S}, V_p(E)) \xrightarrow{\mathrm{loc}} H^i(G_{\mathbb{Q}_l}, V_p(E)).$$

Fact 2.30. There is an exact sequence

$$0 \longrightarrow H^2(G_{\mathbb{Q},S}, V_p(E))^* \longrightarrow H^1(G_{\mathbb{Q},S}, V_p(E)) \xrightarrow{\mathrm{loc}} \bigoplus_{l \in S} H^1(G_{\mathbb{Q}_l}, V_p(E))$$
$$\xrightarrow{\mathrm{loc}^*} H^1(G_{\mathbb{Q},S}, V_p(E)) \longrightarrow \cdots$$

This is known as the *Poitou–Tate exact sequence.*

This begs the natural question: "How do we define the map loc^*?" Note that the first

cohomology group $H^1(G_{Q_l}, V)$ is self dual: $H^1(G_{Q_l}, V) \cong H^1(G_{\mathbb{Q}_l}, V)^*$. So, since

$$\mathrm{loc} : H^1(G_{Q,S}, V_p(E)) \to \bigoplus_{l \in S} H^1(G_{\mathbb{Q}_l}, V_p(E)),$$

the dual map

$$\mathrm{loc}^* : (\bigoplus_{l \in S} H^1(G_{\mathbb{Q}_l}, V_p(E))^* \to H^1(G_{Q,S}, V_p(E))^*.$$

So the image of a global first cohomology group under the composition $\mathrm{loc}^* \circ \mathrm{loc}$ is its own orthogonal complement.

To summarise, this Poitou–Tate duality provides us with a relation between the cohomology of a group module M and its Tate dual $M^\vee(1)$.

2.2.5 The Selmer group and the Shafarevich–Tate group

Let E be an elliptic curve defined over a number field K, and let $G_K = \mathrm{Gal}(\overline{K}/K)$. Suppose $0 \neq m \in \mathcal{O}_K$. The multiplication by m isogeny is surjective on $E(\overline{K})$, so there is a short exact sequence

$$0 \longrightarrow E[m] \longrightarrow E(\overline{K}) \xrightarrow{[m]} E(\overline{K}) \longrightarrow 0$$

Taking G_K-cohomology, we obtain a long exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)[m] & \longrightarrow & E(K) & \xrightarrow{[m]} & E(K) \\ & \searrow & & & & & \\ & & H^1(G_K, E(\overline{K})[m]) & \longrightarrow & H^1(G_K, E(\overline{K})) & \xrightarrow{[m]} & \cdots \end{array}$$

We can rewrite this sequence and extract the *Kummer sequence* for E/K:

$$0 \longrightarrow E(K)/mE(K) \xrightarrow{\kappa} H^1(G_K, E[m]) \xrightarrow{\phi} H^1(G_K, E(\overline{K}))[m] \longrightarrow 0, \tag{2.2}$$

where the connecting homomorphism is the *Kummer map*

$$\begin{aligned} \kappa : E(K) &\to H^1(G_K, E(k)[m]) \\ P &\mapsto ([\zeta] : \sigma \mapsto Q^\sigma - Q) \end{aligned}$$

where $Q \in E(\overline{K})$ satisfies $mQ = P$.

In precisely the same manner, if v is a (finite or infinite) place of K, we may replace K by

the completion K_v in (2.2), which leads to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/mE(K) & \longrightarrow & H^1(G_K, E[m]) & \longrightarrow & H^1(G_K, E(\overline{K}))[m] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{res}_v} & & \downarrow{\scriptstyle \mathrm{res}_v} & & \downarrow{\scriptstyle \mathrm{res}_v} & & \\ 0 & \longrightarrow & E(K_v)/mE(K_v) & \longrightarrow & H^1(G_v, E[m]) & \longrightarrow & H^1(G_{K_v}, E(\overline{K_v}))[m] & \longrightarrow & 0. \end{array}$$

Definition 2.31. The *m-Selmer group* $S_m(E) = S_m(E/K) < H^1(G_K, E[m])$ is given by

$$S_m(E) = \ker\left(H^1(G_K, E[m]) \to \prod_v H^1(G_v, E(\overline{K_v}))\right).$$

Definition 2.32. The *Shafarevich–Tate group* $Ш(E) = Ш(E/K) < H^1(G_K, E(\overline{K}))$ is defined by

$$Ш(E) = \ker\left(H^1(G_K, E(\overline{K})) \to \prod_v H^1(G_v, E(\overline{K}))\right).$$

Thus the Kummer sequence (2.2) restricts to the exact sequence

$$0 \longrightarrow E(K)/mE(K) \longrightarrow S_m(E) \longrightarrow Ш(E)[m] \longrightarrow 0.$$

2.2.6 The Selmer group of E/K

We may now generalise the above constructions by considering the torsion subgroup E_{tors} of $E(\overline{Q})$ and its p-primary subgroups.
Fix an embedding of $K \subset \overline{Q}$ and consider $E[p^\infty] \subset E_{\mathrm{tors}} \subset E(\overline{Q})$, where $E[p^\infty]$ is the p-primary subgroup of E_{tors}; that is, $E_{\mathrm{tors}} = \cup_{n\in\mathbb{N}} E[p^n]$.
The action of $G_K = \mathrm{Gal}\,\overline{\mathbb{Q}}/K$ on E_{tors} allows us to define the Kummer map

$$\begin{aligned} \kappa : E(K) \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} &\to H^1(G_K, E_{\mathrm{tors}}) \\ P \otimes \left(\frac{1}{n} + \mathbb{Z}\right) &\mapsto ([\zeta] : \sigma \mapsto Q^\sigma - Q), \end{aligned}$$

where $Q \in E(\overline{K})$ satisfies $nQ = P$.

Similarly, for v a prime of K, we define the v-adic Kummer map

$$\kappa_v : E(K_v) \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} \to H^1(G_v, E_{\mathrm{tors}}),$$

where K_v denotes the completion of K at v. By embedding $\overline{\mathbb{Q}} \subset \overline{K_v}$, we obtain a restriction map

$$\mathrm{res}_v : H^1(G_K, E_{\mathrm{tors}}) \to H^1(G_v, E_{\mathrm{tors}}).$$

Definition 2.33. The *Selmer group of* E/K is defined by

$$S_E(K) = \ker\left(H^1(G_K, E_{\mathrm{tors}}) \to \prod_v H^1(G_v, E_{\mathrm{tors}})/\operatorname{Im}\kappa_v\right).$$

Definition 2.34. The *Shafarevich–Tate group of* E/K is defined by

$$Ш_E(K) = S_E(K)/\operatorname{Im}\kappa.$$

3 The Coates–Wiles Theorem

3.1 Our Goal

In this section we will utilise the results of the previous two to present an alternative proof of the Coates–Wiles Theorem. It is about time we introduced the statement of the theorem.

Theorem 3.1 (Coates–Wiles)**.** *Suppose E is an elliptic curve defined over a quadratic imaginary field K, with complex multiplication by K, and L-function $L(E, s)$.*
If $L(E, 1) \neq 0$ then $E(K)$ is finite.

By Deuring's Theorem (1.26), we can equivalently say:
Let $\psi : \mathbb{A}_K^* \to \mathbb{C}^*$ be the Grössencharacter attached to E/L.
If $L(1, \overline{\psi}) \neq 0$ then $E(K)$ is finite.

3.2 Bounding Selmer groups

In this subsection we will use the key results of the previous section, namely local Tate duality and the global Poitou–Tate exact sequence, to bound the Selmer groups attached to a certain representation. We follow Darmon and Rotger [D–R, §6.2] closely, clarifying their argument when necessary.

Let E be an elliptic curve, and let W be the trivial representation with coefficients in $\mathbb{Q}$. Fix a prime $p \in \mathbb{Z}$, and an embedding $\mathbb{Q} \in \mathbb{Q}_p$. We have continuous p-adic representations

$$V_p(E) = T_p(E) \otimes \mathbb{Q}_p, \quad W_p = W \otimes_{\mathbb{Q}} \mathbb{Q}_p, \quad V_p(E) \otimes_{\mathbb{Q}_p} W_p.$$

of G_Q, which are $\mathbb{Q}_p$-vector spaces of dimensions 2, 1 and 2 respectively. We wish to bound the Selmer group attached to $V_p(E) \otimes_{\mathbb{Q}_p} W_p$.

Definition 3.2. The *W-isotypic part* of the Mordell–Weil group of E is the $\mathbb{Q}$-vector space

$$E(\mathbb{Q})_{\mathbb{Q}}^W = \mathrm{Hom}(W, E(\mathbb{Q}) \otimes \mathbb{Q}).$$

Restriction to the absolute Galois group $G_{\mathbb{Q}}$ induces an isomorphism

$$\begin{aligned} H^1(\mathbb{Q}, V_p(E) \otimes W_p) &\cong H^1(\mathbb{Q}, V_p(E)) \otimes W_p \\ &= \mathrm{Hom}(W_p, H^1(\mathbb{Q}, V_p(E))) \quad \text{(since } W_p \text{ is self-dual).} \end{aligned} \tag{3.1}$$

Thus the Kummer map

$$\delta : E(\mathbb{Q}) \otimes \mathbb{Q} \to H^1(\mathbb{Q}, V_p(E)) \tag{3.2}$$

gives rise to a homomorphism

$$\delta : E(\mathbb{Q})_Q^{W_p} \to H^1(\mathbb{Q}, V_p(E) \otimes W_p).$$

For each prime $l \in \mathbb{Z}$, the maps (3.1), (3.2) admit local counterparts

$$H^1(\mathbb{Q}_l, V_p(E) \otimes W_p) \cong \mathrm{Hom}(W_p, \oplus_{\lambda|l} H^1(\mathbb{Q}_\lambda, V_p(E)))$$
$$\delta_l : (\oplus_{\lambda|l} E(\mathbb{Q}_\lambda))_{\mathbb{Q}_p}^{W_p} \to H^1(\mathbb{Q}_l, V_p(E) \otimes W_p),$$

for which the following diagram commutes:

$$\begin{array}{ccc} E(\mathbb{Q})_{\mathbb{Q}}^{W} & \xrightarrow{\delta} & H^1(\mathbb{Q}, V_p(E) \otimes W_p) \\ \downarrow \mathrm{res}_l & & \downarrow \mathrm{res}_l \\ (\oplus_{\lambda|l} E(\mathbb{Q}_\lambda))_{\mathbb{Q}_p}^{W_p} & \xrightarrow{\delta_l} & H^1(\mathbb{Q}_l, V_p(E) \otimes W_p). \end{array} \tag{3.3}$$

Definition 3.3. We define the *finite part* of the local cohomology group $H^1(\mathbb{Q}_l, V_p(E) \otimes W_p)$ by $H^1_{\mathrm{fin}}(\mathbb{Q}_l, V_p(E) \otimes W_p) = \mathrm{Im}(\delta_l)$.

Definition 3.4. We define the *singular quotient*:

$$H^1_{\mathrm{sing}}(\mathbb{Q}_p, V_p(E) \otimes W_p) = \frac{H^1(\mathbb{Q}_p, V_p(E) \otimes W_p)}{H^1_{\mathrm{fin}}(\mathbb{Q}_p, V_p(E) \otimes W_p)}$$

Lemma 3.5. *The local cohomology group $H^1(\mathbb{Q}_p, V_p(E) \otimes W_p)$ is a 2-dimensional $\mathbb{Q}_p$-vector space. The finite subspace $H^1_{fin}(\mathbb{Q}_p, V_p(E) \otimes W_p)$ and the singular quotient $H^1_{sing}(\mathbb{Q}_p, V_p(E) \otimes W_p)$ are each 1-dimensional and in perfect duality under the local Tate pairing.*

Proof. Since $V_p(E) \otimes W_p$ is a 2-dimensional Q_p vector space, we know that $H^i(\mathbb{Q}_p, V_p(E) \otimes W_p)$ is finite-dimensional for all $i \geq 0$, and moreover $H^i(\mathbb{Q}_p, V_p(E) \otimes W_p) = 0$ unless $i = 0, 1, 2$. By local duality, $\dim H^0(\mathbb{Q}_p, V_p(E) \otimes W_p) = \dim H^2(\mathbb{Q}_p, V_p(E) \otimes W_p)$, and the Euler characterstic formula reads

$$\dim H^0(\mathbb{Q}_p, V_p(E) \otimes W_p) - \dim H^1(\mathbb{Q}_p, V_p(E) \otimes W_p) + \dim H^2(\mathbb{Q}_p, V_p(E) \otimes W_p) = -2. \tag{3.4}$$

Further, we know $H^0(\mathbb{Q}_p, V_p(E) \otimes W_p) = 0$, so $\dim H^2(\mathbb{Q}_p, V_p(E) \otimes W_p) = 0$, and so the formula (3.4) yields $\dim H^1(\mathbb{Q}_p, V_p(E) \otimes W_p) = 2$.
It is clear from the definition that

$$2 = \dim H^1(\mathbb{Q}_p, V_p(E) \otimes W_p) = \dim H^1_{\mathrm{fin}}(\mathbb{Q}_p, V_p(E) \otimes W_p) + \dim H^1_{\mathrm{sing}}(\mathbb{Q}_p, V_p(E) \otimes W_p)$$

and both $\dim H^1_{\text{fin}}(\mathbb{Q}_p, V_p(E) \otimes W_p) \neq 0$ and $\dim H^1_{\text{sing}}(\mathbb{Q}_p, V_p(E) \otimes W_p) \neq 0$, so

$$\dim H^1_{\text{fin}}(\mathbb{Q}_p, V_p(E) \otimes W_p) = \dim H^1_{\text{sing}}(\mathbb{Q}_p, V_p(E) \otimes W_p) = 1.$$

□

Now consider the restriction map

$$\text{res}_p : H^1(\mathbb{Q}, V_p(E) \otimes W_p) \to H^1(\mathbb{Q}_p, V_p(E) \otimes W_p)$$

from the global to the local cohomology at p.

Definition 3.6. The *residue map at p* is the composition

$$\partial_p : H^1(\mathbb{Q}, V_p(E) \otimes W_p) \to H^1_{\text{sing}}(\mathbb{Q}_p, V_p(E) \otimes W_p)$$

of res_p with the natural projection to the singular quotient.

Proposition 3.7. *If the map ∂_p is surjective, then the map*

$$res_p : H^1_{fin}(\mathbb{Q}, V_p(E) \otimes W_p) \to H^1_{fin}(\mathbb{Q}_p, V_p(E) \otimes W_p) \tag{3.5}$$

is the zero map.

Proof. □

Proposition 3.8. *If the residue map ∂_p attached to the representation $V_p(E) \otimes W_p$ is a surjective map of $\mathbb{Q}_p$-vector spaces, then $E(\mathbb{Q})^W_{\mathbb{Q}} = 0$.*

Proof. By Proposition 3.7, the map res_p of (3.5) is the zero map, and so, since the diagram (3.3) is commutative, this implies that the natural map

$$\text{res}_p : E(\mathbb{Q})^W_{\mathbb{Q}} \to ((\oplus_{\mathfrak{p}|p} E(\mathbb{Q}_{\mathfrak{p}})) \otimes \mathbb{Q}_p)^W$$

is the zero map. This in turn implies that the vector space $E(\mathbb{Q})^W_{\mathbb{Q}}$ has trivial image in the group $\oplus_{\mathfrak{p}|p} E(\mathbb{Q}_{\mathfrak{p}}) \otimes \mathbb{Q}$ of local points. However, W is a rational representation (namely, the trivial representation) and hence admits a $\mathbb{Q}$-basis consisting of elements of $E(\mathbb{Q})$. Since the natural map $E(\mathbb{Q}) \to \oplus_{\mathfrak{p}|p} E(\mathbb{Q}_{\mathfrak{p}})$ is injective modulo torsion, it follows that $\dim_{\mathbb{Q}} E(\mathbb{Q})^W_{\mathbb{Q}} = 0$, and therefore $E(\mathbb{Q})^W_{\mathbb{Q}} = 0$. □

3.3 Finishing argument

Our goal is in sight; we have almost reached a proof of the Coates–Wiles Theorem. The final step is some way beyond the scope of this project in terms of difficulty, so we merely state the result, quoting directly from Kato [Ka, §15] (explanation will follow):

Theorem 3.9 (Kato)**.** *Fix a quadratic imaginary field K and an embedding $K \hookrightarrow \mathbb{C}$. Let $r \geq 1$ and let ψ be a Hecke character of K of type $(-r, 0)$. Let p be a prime number, let $\mathfrak{f}$ be a non-zero ideal of $\mathcal{O}_K$ contained in the conductor of ψ, let K' be a finite extension of K contained in $K(p^\infty\mathfrak{f})$, and let $\gamma \in V_L(\psi)$. Then the image of $z_{p^\infty\mathfrak{f}}$ under*

$$H^1_{p^\infty\mathfrak{f}}(\mathbb{Z}_p(1)) \xrightarrow{\gamma} H^1_{p^\infty\mathfrak{f}}(\mathbb{Z}_p(1)) \otimes V_{L_\lambda}(\psi) \xrightarrow{\sim} H^1_{p^\infty\mathfrak{f}}(V_{L_\lambda}(\psi)(1)) \to$$
$$H^1(\mathcal{O}_{K'}[1/p], V_{L_\lambda}(\psi)(1)) \xrightarrow{exp^*} D^1_{\mathrm{dR}}(K' \otimes \mathbb{Q}_p, V_{L_\lambda}(\psi)) \cong (S(\psi) \otimes_L L_\lambda) \otimes_K K' \qquad (3.6)$$

is an element of $S(\psi) \otimes_K K'$ whose image under

$$\sum_{\sigma \in \mathrm{Gal}(K'/K)} \chi(\sigma)\, \mathrm{per}_\psi \circ \sigma : S(\psi) \otimes_K K' \to V_{\mathbb{C}}(\psi)$$

coincides with $L_{p\mathfrak{f}}(\overline{\psi}, \chi, r) \cdot \gamma$ for any homomorphism $\chi : \mathrm{Gal}(K'/K) \to \mathbb{C}^\times$.
Here $L_{p\mathfrak{f}}(\overline{\psi}, \chi, s)$ denotes $\sum_{\mathfrak{a}} \overline{\psi}(\mathfrak{a})\chi(\mathfrak{a})N(\mathfrak{a})^{-s}$ in which $\mathfrak{a}$ ranges over all ideals of $\mathcal{O}_K$ which are prime to $p\mathfrak{f}$.

Proof. See Kato, Proposition 15.9 [Ka, pp. 258–259]. □

This theorem provides the precise link between the values of the L-function and the rational points of the elliptic curve needed to prove the Coates–Wiles theorem. Some of the notation here is difficult to grasp, so let us rewrite the diagram 3.6 in a more simplistic form: let L/K be an abelian extension of K, unramified outside p, with $L \subset K[E_{p^\infty}]$. Then

$$L^\times \xrightarrow{\kappa} \varprojlim_L H^1(L, \mathbb{Q}_p(1)) \cong \varprojlim_L H^1(L, \psi) \longrightarrow H^1(K, \psi) \cong H^1(\mathbb{Q}, V_p(E)).$$

The last isomorphism requires some elaboration; the following is a standard result in group cohomology:

Lemma 3.10 (Shapiro)**.** *Let H be a subgroup of G and M a representation of H. Then for all $i \geq 0$ we have*

$$H^i(G, \mathrm{Ind}_H^G M) = H^i(H, M).$$

Proof. See Neukirch–Schmidt–Wingberg, Proposition 1.6.3 [NSW, pp. 59–60]. □

So it remains to show [7]

Proposition 3.11. *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by the field K. Then*

$$V_p(E) \cong \mathrm{Ind}_{G_K}^{G_\mathbb{Q}} \psi,$$

where ψ is the Grössencharacter associated to $E/\mathbb{Q}$.

[7] An adaptation of Kato [Ka §15.10].

Proof. As a representation of $G_{\mathbb{Q}}$, $V_p(E)$ is isomorphic to the representation

$$V_{\tilde{p}}(\psi) = V_p(\psi) \oplus \iota V_p(\psi)$$

induced from the representation $V_p(\psi)$ of the subgroup G_K of $G_{\mathbb{Q}}$. Here $\iota \in G_{\mathbb{Q}}$ denotes complex conjugation, and the action of $\sigma \in G_{\mathbb{Q}}$ on $V_{\tilde{p}}(\psi)$ sends

$$(x, \iota y) \mapsto \begin{cases} (\sigma(x), \iota(\iota\sigma\iota)(y)) & \text{if } \sigma \in G_K \\ ((\iota\tau\iota)(y), \iota\tau(x)) & \text{if } \sigma = \iota\tau \text{ with } \tau \in G_K. \end{cases}$$

To see this □

Bibliography

[D–R] H. Darmon and V. Rotger, Diagonal Cycles and Euler Systems II: The Birch and Swinnerton-Dyer conjecture for Hasse–Weil–Artin L-functions, 1st draft.

[I–R] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, GTM 84, Springer-Verlag, New York, 1990.

[Ka] K. Kato, p-adic Hodge Theory and Values of Zeta Functions of Modular Forms, Astérisque 295 (2004), 117–290.

[NSW] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, Grundlehren der Mathematischen Wissenschaften 323, Springer-Verlag, Berlin, 2000.

[Ru] K. Rubin, Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton-Dyer, Invent. Math. 64 (1981), 455–470.

[Si 1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, New York, 1986.

[Si 2] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM 151, Springer-Verlag, New York, 1994.

[Ta] J. Tate, Galois Cohomology, Arithmetic algebraic geometry (Park City, UT, 1999), 465–479, AMS, Providence, RI, 2001.