## Explicit class field theory over quadratic fields

The aim of this study group is twofold.

In the first half, we will introduce beautiful and classical results from the theory of *complex* multiplication (CM), and explain a little why they give an imaginary quadratic analogue of the Kronecker–Weber theorem, that is, an explicit description of class field theory over imaginary quadratic fields. We also discuss the closely-related work of Gross–Zagier: in particular, we will have talks on Heegner points on elliptic curves, and their role in proofs of cases of BSD; and on the arithmetic properties of special values of the $j$-function (so-called 'singular moduli'). As we shall see, all of these ideas stem from the study of quadratic points in the (complex) upper and lower half-planes $\mathcal{H} := \mathbf{C}\backslash\mathbf{R}$, that is, numbers $\tau \in \mathcal{H}$ such that $\mathbf{Q}(\tau)$ is an imaginary quadratic field.

In the second half, we explore analogues with *real* multiplication (RM), due to the remarkable work of Henri Darmon and his collaborators. Fundamentally we cannot pursue the same approach as above: if $\mathbf{Q}(\tau)$ is a *real* quadratic field, then $\tau \in \mathbf{R}$, so does *not* lie in the upper half-plane. Instead, Darmon's idea was to replace the complex upper half-plane with the $p$-adic upper half-plane $\mathbf{C}_p\backslash\mathbf{Q}_p$. Now if $\mathbf{Q}(\tau)$ is a real quadratic field with $p$ inert, then $\tau \neq \mathbf{Q}_p$, so $\tau$ gives a non-trivial point in $\mathcal{H}_p$. Using this one can try to find *$p$-adic* RM analogues of the complex CM theory. We will have talks on Tate uniformisation of curves, the Bruhat–Tits tree (which is the 'skeleton' of the upper half-plane), Darmon's theory of Stark–Heegner points (conjectural points on elliptic curves that are real quadratic analogues of Heegner points), and Darmon–Vonk's theory of real quadratic singular moduli, a conjectural version of explicit class field theory over real quadratic fields.

There is strong overlap between the material in this study group and all three of the study groups last year (Class Field Theory, modular forms, and Shimura varieties). For those who had not started here yet, hopefully the relevant material will be summarised again here, but necessarily some things will be terse (e.g. there will not be time to say much about modular curves and modular forms, which will be used in the sections on Heegner and Stark–Heegner points).

Our main references will be:

**Dar20** Lecture notes (by Francesc Gispert) of Darmon's course in Montreal, Fall 2020, found at `https://www.math.mcgill.ca/darmon/courses/20-21/cm/francesc-notes.pdf`

**Sil94** Silverman's book 'Advanced topics in the arithmetic of elliptic curves'

**Dar01** Darmon's book 'Rational points on modular elliptic curves', found at `https://www.math.mcgill.ca/darmon/pub/Articles/Research/36.NSF-CBMS/chapter.pdf`

**Talk 1: CM elliptic curves.** 15th Oct 2021

An elliptic curve $E/\mathbf{C}$ has *complex multiplication* if its endomorphism ring is larger than $\mathbf{Z}$. In this case, it turns out that $\mathrm{End}(E)$ is an order (lattice) in an imaginary quadratic field $K$, and we say $E$ has *CM by $K$*. The existence of these extra endomorphisms force $E$ to have all sorts of beautiful arithmetic consequences; in particular, its $j$-invariant is algebraic, $E$ has a model over the number field generated by $K$ and $j(E)$, and there is a transitive action of the class group of $K$ on the isomorphism classes of elliptic curves with CM by $K$.

This talk should describe the theory of CM elliptic curves, including definitions and basic properties. It should describe (without proofs) the transitive action of the class group of $K$ on the isomorphism classes of elliptic curves with CM by $K$.

*References:* [Dar20, §3.1-3.3]

**Talk 2: Explicit CFT for IQF.** 22nd Oct 2021

The *Kronecker–Weber theorem* says that every abelian extension of $\mathbf{Q}$ is contained in a cyclotomic field. This gives a complete explicit version of Class Field Theory over $\mathbf{Q}$. In fact, CM elliptic curves give a similarly explicit theory over any imaginary quadratic field. If $E$ is an elliptic curve with CM by $K$, then one can show its Hilbert class field is $K(j(E))$, and moreover that any abelian extension of $K$ is contained in the extension of $K(j(E))$ generated by the co-ordinates of all torsion points in $E(\overline{\mathbf{Q}})$.

This talk should sketch these results.

*References:* [Sil94, §II.3–§II.5]

**Talk 3: Heegner Points.** 29th Oct 2021

*Heegner points* are global points on elliptic curves. Loosely, they are defined as follows. Given an elliptic curve $E$, the modularity theorem gives a surjective map $m : X_0(N) \to E$ from the modular curve of level $X_0(N)$. This modular curve is a moduli space of elliptic curves with level $N$ structure. Via CM theory, we can write down a supply of elliptic curves with remarkable arithmetic properties, giving 'nice' points in $X_0(N)$; and their image under $m$ gives a supply of points on $E$. Moreover, a celebrated theory of Gross–Zagier relates the height of such a point to the derivative of $L(E, s)$ evaluated at $s = 1$, and this was of profound importance in Kolyvagin's solution of BSD in analytic rank 1.

This talk should give an overview of these topics, including some consequences for the BSD conjecture.

*References:* [Dar01, §3]

**Talk 4: Singular moduli and the class number 1 problem.** 5th Nov 2021

The $j$-function is a meromorphic modular function of weight 0; it computes the $j$-invariant of elliptic curves. Prior to their work on Heegner points, Gross and Zagier worked on *singular moduli*, values of the $j$-function at imaginary quadratic points of the upper half-plane. These values satisfy wonderful arithmetic properties: for example, certain products of differences of singular moduli lie in $\mathbf{Z}$, and have surprising factorisations.

In a different but closely related direction, one can study the famous class number 1 problem by using singular moduli, by studying algebraic points on modular curves.

This talk should give an overview of these topics.

*References:* [Dar20, §3.9, §3.10]

**Talk 5: Tate uniformisation of elliptic curves.** 12th Nov 2021

In a course on elliptic curves, one sees that any complex elliptic curve can be written as a quotient of $\mathbf{C}$ by a lattice. In the 1960s, Tate found an analogue for elliptic curves defined over $\mathbf{Q}_p$. Since any additive subgroup of $\mathbf{Q}_p$ is dense, one cannot no longer consider quotients of $\mathbf{Q}_p$ by lattices. Instead, one can observe that the exponential map sends $\mathbf{C}/(\mathbf{Z} + \tau\mathbf{Z})$ to $\mathbf{C}^\times/q^{\mathbf{Z}}$, for $q = e^{2\pi i\tau}$, and this has a good $p$-adic analogue. Indeed, Tate showed that any elliptic curve over $\mathbf{Q}_p$ with split multiplicative reduction is isomorphic to $\mathbf{Q}_p^\times/q^{\mathbf{Z}}$, for an explicit $p$-adic number $q$ closely related to $j(E)$.

This talk should describe the key properties of Tate uniformisation of $p$-adic elliptic curves.

*References:* [Sil94, §V]

**Talk 6: The Bruhat–Tits tree.** 19th Nov 2021

The $p$-adic upper half-plane $\mathcal{H}_p := \mathbf{C}_p \backslash \mathbf{Q}_p$ is a $p$-adic analytic analogue of the usual upper half-plane. Morally, one could consider $p$-adic modular forms as being $p$-adic analytic functions on $\mathcal{H}_p$, in much the same way as classical modular forms are holomorphic functions on $\mathcal{H}$.

The geometry of $\mathcal{H}_p$ can be modelled more simply using a combinatorial object known as the *Bruhat–Tits tree*, a connected graph on which $\mathrm{PGL}_2(\mathbf{Q}_p)$ acts transitively. This talk should describe the definition and basic properties of the Bruhat–Tits tree.

*References:* [Dar01, §5]

**Talks 7 & 8: Stark–Heegner points I.** 26th Nov 2021, 3rd Dec 2021

*Stark–Heegner points* are real quadratic analogues of the Heegner points from Talk 3. Defined by Darmon, they use Tate uniformisation of a $p$-adic elliptic curve; the idea is to write down naturally defined 'arithmetic' elements of $\overline{Q}_p^\times$, and then project them into $E(\overline{\mathbf{Q}}_p) = \overline{\mathbf{Q}}_p^\times / q^{\mathbf{Z}}$. To write down these arithmetic elements, Darmon defines a theory of $p$-adic integration for modular forms using the Bruhat–Tits tree, and applies it to the modular form $f_E$ attached to $E$ to construct his Stark–Heegner points. Unlike Heegner points, these points are only locally defined; but Darmon has conjectured that they are in fact global points (i.e. their coefficients lie in a number field) and satisfy reciprocity laws analogous to classical Heegner points. There is a huge wealth of computational evidence for his conjectures.

These talks should describe the Darmon's construction and conjectures. The first talk will focus on modular symbols and modular forms on the Bruhat–Tits tree. The second talk would be a bit more advanced, defining the theory of $p$-adic integration and giving the construction/stating the conjectures.

*References:* [Dar01, §9.1, §9.2] (talk 7) and [Dar01, §9.3–§9.5] (talk 8)

**Talk 9: Real quadratic singular moduli.** 10th Dec 2021

Whilst Darmon's ideas surrounding $p$-adic integration and Stark–Heegner points have generated decades worth of research, his original motivation was to find a real quadratic analogue of the explicit Class Field Theory given by CM (talk 2). In recent years, in joint work with Jan Vonk, he has found a good candidate for this theory via *real quadratic singular moduli*. Whilst the direct analogue of 'values of the $j$-function' does not yield useful arithmetic objects in the real quadratic setting, Darmon and Vonk interpreted this as a (rigid meromorphic) '0-cocycle' and instead asked what happens when one instead studies '1-cocycles'. They found a way of writing down good (local) analogues of singular moduli over real quadratic fields, and conjectured these quantities are global, generating (ring) class fields of real quadratic fields. Again, they have a wealth of computational evidence for these conjectures.

This talk will be considerably harder to prepare, and will probably be more a seminar-style talk, describing the referenced paper of Darmon and Vonk.

*References:* Henri Darmon and Jan Vonk, *Singular moduli for real quadratic fields: a rigid analytic approach*, Duke Math. J., 2021.