LECTURE 28: COMPLEX MULTIPLICATION

LARRY ROLEN, VANDERBILT UNIVERSITY, FALL 2020

> The theory of complex multiplication is not only the most beautiful part of mathematics but also of the whole of science.
>
> David Hilbert

1. Elliptic Curves Picture

We have hinted a number of times throughout the class about the theory of **Complex Multiplication**, or CM for short. CM theory connections elliptic curves, algebraic number theory, and modular forms. We will describe the key aspects of this theory. An excellent exposition of this is found in Zagier's chapter in the 1-2-3 of Modular Forms. We will closely follow his exposition in most of this document.

We begin with the story for elliptic curves, where the term "complex multiplication" comes from. Let $E/\mathbb{C}$ be an elliptic curve. Then $E \cong \mathbb{C}/\Lambda$ for some lattice Λ, as we've seen. Given another curve $E' \cong \mathbb{C}/\Lambda'$, and a $\lambda \in \mathbb{C}$ such that

$$\lambda\Lambda \subseteq \Lambda',$$

the multiplication by λ map sends $E \to E'$.

In the special case when $\Lambda = \Lambda'$, so that we require $\lambda\Lambda \subseteq \Lambda$, we get an **endomorphism** $E \to E$. What λ can we perform "multiplication" with to obtain an endomorphism? It is clear that if $\lambda \in \mathbb{Z}$, then we have $\lambda\Lambda \in \Lambda$. However, there are never any other *real* values λ which work. Sometimes, there are additional complex numbers we can multiply by, $\lambda \in \mathbb{C} \setminus \mathbb{R}$. **In this case, we say the curve has CM.** In short, this means that the curve has an endomorphism ring strictly larger than $\mathbb{Z}$. If its not $\mathbb{Z}$, then it turns out its what we call an *order* in an imaginary quadratic field.

Example. *For $\alpha \in \mathbb{C}^\times$, consider the elliptic curve $\mathbb{C}/(\alpha \cdot \mathbb{Z}[i])$. Then multiplication by i keeps you in the same lattice, and so the curve has CM. The Weierstrass equation of this curve is*

$$E\colon y^2 = 4x^3 - ax.$$

We can write down the extra endomorphism here as the map sending

$$x \mapsto -x, \quad y \mapsto -iy,$$

which is an order 4 endomorhpism. This recovers the example of the congruent number elliptic curve, which explains why we said that curve has CM.

2. CM points and singular moduli

I have briefly mentioned CM points before. How do these relate to elliptic curves? We know that elliptic curves correspond to points in $\Gamma(1)\backslash\mathbb{H}$, via

$$\Gamma(1)\tau \leftrightarrow [\mathbb{C}/\Lambda_\tau], \ \Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}.$$

If we have an elliptic curve with CM, we can consider the corresponding point in $\Gamma(1)\backslash\mathbb{H}$, or a representative of it, say in the fundamental domain. The corresponding points are the **CM points**. For instance, in the previous example, the point corresponding to the CM elliptic curves we constructed in the last example is the CM point $\tau = i$.

An equivalent definition: it turns out that these are simply the algebraic integers in imaginary quadratic fields which lie in the upper half plane (an algebraic integer is the root of a monic integer polynomial).

Values of modular forms at these CM points are "nice." For instance, we'll see that

$$j(\mathrm{CM}) \in \overline{\mathbb{Q}},$$

that is, that $j(\tau)$ evaluated at a CM point is algebraic. These special values are called **singular moduli**. A fun fact which Schneider proved is that if $j(\tau)$ is algebraic for an *algebraic* input τ, then in fact τ *must* be a CM point. So at least for "nice" numbers, there are no other values of j which are also nice in the sense of being algebraic. Thus, they are indeed very special, or "singular."

These singular moduli are also important numbers, which generate so-called **class fields**, as we shall see below.

3. CM Modular forms

There is also a notion of a CM modular form, which we won't need as much. However, we'll note that in studying the Congruent Number Problem, we pointed out that the L-functions of the Congruent Number Curve had a special representation as a Dirichlet series for a so-called Hecke character of $\mathbb{Z}[i]$, which is also the L-function of a modular form that's a theta series for that character. A theorem of Ribet states that a newform has CM (whatever the precise definition is) if and only if f is a theta series for such a character. So this can be considered as a prototypical example.

4. CM Number Fields

We have already seen that imaginary quadratic fields play a role in CM theory. These are basic examples of **CM number fields**. This definition requires a bit of algebraic number theory, so if you haven't seen the following terms, don't worry as we won't need this definition. A CM number field (note: a number field is just a finite extension of $\mathbb{Q}$) is a quadratic extension K/F where F is a totally real field and K is totally imaginary. Totally real means that all embeddings of the field into $\mathbb{C}$ are contained in $\mathbb{R}$, and totally imaginary means that none of the complex embeddings are.

Example. *For $K = \mathbb{Q}(\sqrt{D})$ with $D < 0$, we have that $F = \mathbb{Q}$ is totally real, and K is totally imaginary. Thus, $\mathbb{Q}(\sqrt{D})$ is a CM field.*

Example. *The next most important example is the* **cyclotomic field** *$K = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity such as $e(\frac{1}{n})$. This is a quadratic extension of*

$F = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, which happens to be a totally real field. However, one can also show that K is totally imaginary, so is CM (if you were in my algebra class last semester, we discussed this example in the algebraic number theory unit). The cyclotomic field is a quadratic extension of F since it is obtained by adjoining a square root of $\zeta_n^2 + \zeta_n^{-2} - 2 = (\zeta_n - \zeta_n^{-1})^2$.

5. First proofs

Some of the terminology and connections to different subjects out the way, let's dive into proving key results in the theory.

Theorem. *If τ is a CM point, then $j(\tau)$ is algebraic.*

Proof. If τ is a CM point, then it satisfies a quadratic equation over $\mathbb{Z}$, say of the form

$$A\tau^2 + B\tau + C = 0.$$

Then the matrix

$$M = \begin{pmatrix} B & C \\ -A & 0 \end{pmatrix}$$

fixes τ. To check this, note that we want

$$M\tau = \frac{B\tau + C}{-A\tau} = \tau,$$

which is equivalent to $B\tau + C = -A\tau^2$. Clearly this follows from the original quadratic equation satisfied by τ. The determinant of M is positive, as $\tau \in \mathbb{H}$ implies that $B^2 - 4AC < 0$, which implies that $AC > 0$. Thus, M acts on $\mathbb{H}$ in addition to fixing τ (and, in the language of the last set of notes, M is an elliptic matrix).

Consider the two modular functions $j(\tau)$ and $j(M\tau)$. Since the latter can be written using the slash operator as $j|_0 M$, by our earlier work this lies in $M_0^!(\Gamma(1) \cap M^{-1}\Gamma(1)M)$. The function $j(\tau)$ is also in this space. But the space of weight 0 modular forms there (recall: these are also called modular functions) cannot have two algebraically independent elements.

To see why, suppose that Γ is a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ and that $\Gamma\backslash\mathbb{H}$ has finite volume V (with respect to the hyperbolic measure $d\mu = dudvv^{-2}$). Then a valence-formula type argument generalizing what we did to compute dimensions of modular form spaces in level one implies that

$$\dim M_k(\Gamma) \leq \frac{kV}{4\pi} + 1.$$

(To compare with the $\mathrm{SL}_2(\mathbb{Z})$ case, note that an elementary integral computation shows that the volume of the fundamental domain in this case is $\pi/3$, so that the dimension of M_k is bounded by $k/12 + 1$ in this formula.) We only really need how quickly this dimension grows asymptotically as a function of k. Thus, any three holomorphic modular forms on Γ are algebraically dependent, as if there were three algebraically independent

ones, then we'd have at least the number of monomials in these three forms of total weight k living in the space of weight k modular forms. But the number of such monomials is $\gg k^2$, i.e., worse than the linear in k bound on the dimension above. Any modular *function* is a quotient of two modular forms, which then implies that any *two* modular functions are algebraically dependent. (Note: This is an instance of the general fact that there are at most n algebraically independent functions on a variety of dimension n, and modular functions are functions on a modular curve $\Gamma\backslash\mathbb{H}$.)

Since there is an algebraic depdendency between $j(\tau)$ and $j(M\tau)$, there is a non-zero polynomial $P(X,Y)$ such that

$$P(j(M\tau), j(\tau)) = 0.$$

By comparing Fourier expansions, we can make P have $\mathbb{Q}$-rational coefficients.

Exercise 1. *Show this.*

We can also assume that $P(X,X) \neq 0$. For, if a power of $X - Y$ divided P, then we can simply delete it as it doesn't affect the relation $P(j(M\tau), j(\tau)) = 0$, since $j(M\tau)$ is not identically equal to $j(\tau)$ as a function.

Thus, $j(\tau)$ is a root of $P(x,x)$, a non-zero polynomial with rational coefficients. This implies that $j(\tau)$ is algebraic, as desired. □

Similarly, by the same proof, one can show the following.

Theorem. *If f is a modular function on a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ with algebraic Fourier coefficients at $i\infty$, then $f(\tau) \in \overline{\mathbb{Q}}$ for any CM point τ.*

It is natural to ask the following.

Questions. *What number field do the values $f(\tau)$ in the last theorem live in? How does the Galois group of the field they live in over the rationals act on them?*

We'll soon see what number fields arise from such constructions. The answer to the second question is that Galois conjugates of a singular modulus are other singular moduli.

We can give a more precise statement of the above theorem on algebraicity of singular moduli, which will be useful. Specifically, we can choose a single polynomial relation between $j(\tau)$ and $j(M\tau)$ for **all** CM points of a given discriminant (the discriminant of a CM point is the minimal discriminant of an integral quadratic polynomial its a root of).

Theorem. *Let $m \in \mathbb{N}$. Then there is a polynomial*

$$\Psi_M(X,Y) \in \mathbb{Z}[X,Y],$$

symmetric up to a sign in X, Y, of degree $\sigma_1(m)$ in both variables, such that

$$\Psi_m(j(M\tau), j(\tau)) = 0$$

for all integral matrices M of determinant m.

Proof. Let

$$\mathcal{M}_m := \left\{ M \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}) \;\middle|\; \det(M) = m \right\}.$$

As we saw when we studied Hecke operators, $\mathrm{SL}_2(\mathbb{Z})$ acts on M_m, and a set of representatives for $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{M}_m$ is given by

$$\mathcal{M}_m^* := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \;\middle|\; a, b, d \in \mathbb{Z},\ ad = m,\ 0 \le b < d \right\}.$$

The number of representatives in this set is

$$\#\mathcal{M}_m^* = \sum_{ad=m} d = \sigma_1(m).$$

We now claim that there is a polynomial $\Psi_m(X, Y)$ for which

$$\prod_{M\in\mathcal{M}_m^*} (X - j(M\tau)) = \Psi_m(X, j(\tau)).$$

The left hand side is well-defined as a product over $\Gamma(1)\backslash\mathcal{M}_m$, as $j(M\tau)$ only depends on the class of M in $\Gamma(1)\backslash\mathcal{M}_m$. It is invariant under $\Gamma(1)$, as $\mathcal{M}_m$ is invariant under right multiplication by $\Gamma(1)$. Iss also clearly a polynomial of degree $\sigma_1(m)$ in X. Moreover, the left hand side of the above, as a polynomial in X, has coefficients which are holomorphic functions in τ of at worst (linear) exponential growth at $i\infty$, as each coefficient is itself a polynomial in the $j(M\tau)$. Thus, each coefficient is a weakly holomorphic modular function in $M_0^!$, and hence by what we proved a long time ago about level 1 modular functions, is a polynomial in $j(\tau)$. This shows that $\prod_{M\in\mathcal{M}_m^*} (X - j(M\tau)) = \Psi_m(X, j(\tau))$ for some polynomial Ψ_m.

We'll now show that Ψ_m has *integer* coefficients. For this, we'll use our explicit choice of representatives $\mathcal{M}_m^*$. Firstly, write

$$j(\tau) = q^{-1} + 744 + 196884q + \ldots =: \sum_{n\ge -1} c(n) q^n.$$

Then we have

$$\Psi_m(X, j(\tau)) = \prod_{M\in\mathcal{M}_m^*} (X - j(M\tau)) = \prod_{\substack{ad=m \\ d>0}} \prod_{b=0}^{d-1} \left(X - j\left(\frac{a\tau + b}{d}\right)\right)$$

$$= \prod_{\substack{ad=m \\ d>0}} \prod_{b \pmod d} \left(X - \sum_{n\ge -1} c(n) \zeta_d^{bn} q^{\frac{an}{d}} \right),$$

where $\zeta_a := e(1/a)$ (recall, we saw similar computations when discussing Hecke operators). The last expression inside the big parentheses is in $\mathbb{Z}[\zeta_d][X]((q^{\frac{1}{d}}))$, i.e., the terms in the sum are in the ring of Laurent series over $q^{\frac{1}{d}}$ with coefficients in $\mathbb{Z}[\zeta_d]$. To show that we really have something defined over $\mathbb{Z}$, we use a bit of Galois theory. Galois theory implies that to check our elements are in $\mathbb{Q} \cap \mathbb{Z}[\zeta_d] = \mathbb{Z}$, we just have to check

its fixed by the Galois group of $\mathbb{Q}(\zeta_d)$, which it turns out consists of the power maps sending

$$\zeta_d \mapsto \zeta_d^r$$

extended to all elements of $\mathbb{Q}(\zeta_d)$ in the natural way, for all choices of powers $r \in (\mathbb{Z}/d\mathbb{Z})^\times$. Explicitly, this operation, in the product above, replaces b by br, but as b ranges mod d, so does br range over a complete set of residues modulo d. Thus,

$$\prod_{b \pmod d} \left(X - \sum_{n \geq -1} c(n) \zeta_d^{bn} q^{\frac{an}{d}} \right) \in \mathbb{Z}[X]((q)) \implies \Psi_m(X, j(\tau)) \in \mathbb{Z}[X]((q)).$$

Now this is a polynomial in j, which has integral Fourier coefficients and leading coefficient q^{-1}, and so

$$\Psi_m(X, j(\tau)) \in \mathbb{Z}[X, j(\tau)].$$

The symmetry (up to sign) holds since

$$\begin{cases} \tau' = M\tau \\ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_m \end{cases} \iff \begin{cases} \tau = M'\tau' \\ M' = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in \mathcal{M}_m. \end{cases}$$

□

Example. *Let $m = 2$. Then we have*

$$\prod_{M \in \mathcal{M}_2^*} (X - j(\tau)) = \left(X - j\left(\frac{\tau}{2}\right)\right)\left(X - j\left(\frac{\tau+1}{2}\right)\right)(X - j(2\tau)).$$

Say that this is $X^3 - A(\tau)X^2 + B(\tau)X - C(\tau)$. Then

$$A(\tau) = j\left(\frac{\tau}{2}\right) + j\left(\frac{\tau+1}{2}\right) + j(2\tau) = \left(q^{-\frac{1}{2}} + 744 + \ldots\right) + \left(-q^{-\frac{1}{2}} + 744 + \ldots\right) + \left(q^{-2} + 744 + \ldots\right)$$

$$= q^{-2} + 2232 + \ldots.$$

This leading part of the expansion (we call the non-positive terms the **principal part***) is enough to determine it as a polynomial in $j(\tau)$. Specifically, after a little linear algebra we find that*

$$A(\tau) = j(\tau)^2 - 1488j(\tau) + 16200 + o(1),$$

where $o(1)$ means a function tending to 0 as $\tau \to i\infty$. As $A(\tau)$ is holomorphic on $\mathbb{H}$ and is $\mathrm{SL}_2(\mathbb{Z})$-invariant, we have precisely

$$A = j^2 - 1488j + 16200.$$

Similarly, one can compute that

$$B = 1488j^2 + 40773375j + 8748000000$$

and

$$C = -j^3 + 162000j^2 - 8748000000j + 157464000000000.$$

Thus,

$$\Psi_2(X,Y) = -X^2Y^2+X^3+1488X^2Y+1488XY^2+Y^3-162000X^2+40773375XY-162000Y^2$$
$$+8748000000X + 8748000000Y - 157464000000000$$

Clearly, these polynomials grow very quickly! However, one can compute these sorts of polynomials for other modular functions to obtain polynomials with much smaller coefficients which will have the same applications that these polynomials do to algebraic number theory that we'll talk about. In applications to cryptography for example, the smallness of coefficients of the resulting polynomials is critical in implementations.

For the algebraicity of CM-values of $j(\tau)$, as above, we can use that

$$\Psi_m(j(\tau), j(\tau)) = 0.$$

Here, the restriction to the diagonal is simpler, and in fact very nice. For instance, when $m = 2$, we get

$$\Psi_2(X,X) = -(X-8000)(X+3375)^2(X-1728).$$

Here we obtain our number 1728 that occasionally has popped up for us, here arising due to the fact that $j(i) = 1728$. As you may expect by now, this nice formula isn't a coincidence.

Remark. *In general, $\Psi_m(X,Y)$ isn't irreducible (if you want to study an algebraic number as a root of a polynomial, its preferable to have it as a root of an irreducible one). However, it turns out that one can write*

$$\Psi_m(X,Y) = \prod_{r^2|m} \Phi_{\frac{m}{r^2}}(X,Y),$$

where Φ_m has the same definition as Ψ_m but with $\mathcal{M}$ replaced by the set of primitive matrices of determinant m, and the $\Phi_m(X,Y)$ are then irreducible.

If m is a square, then $\Psi_m(X,X) = 0$, as $\Psi_m(X,y)$ contains the factor $\Psi_1(X,X) = (X-Y)$. Thus, the restriction to the diagonal is not interesting in such cases. However, for non-square values of m, we obtain the following.

Theorem. *If m is not a square, then $\Psi_m(X,X)$ is (up to multiplying by ± 1) a monic polynomial of degree*

$$\sigma_1(m)^+ := \sum_{d|m} \max(d, m/d).$$

Proof. Using the difference of d-th powers formula

$$\prod_{b \pmod d} \left(X - \zeta_d^b Y\right) = X^d - Y^d,$$

we obtain

$$\Psi_m(j(\tau), j(\tau)) = \prod_{ad=m} \prod_{b \pmod d} \left(j(\tau) - j\left(\frac{a\tau + b}{d}\right)\right) = \prod_{ad=m} \prod_{b \pmod d} \left(q^{-1} + \zeta_b^{-d} q^{-\frac{a}{d}} + o(1)\right)$$
$$= \prod_{ad=m} \left(q^{-d} - q^{-a} + \ldots\right) \sim \pm q^{-\sigma_1^+(m)}.$$

Here, recall that the asymptotic to symbol $\sim$ means that the ratio of both sides tends to 1, here taken in the limit as $\tau \to i\infty$. This proves the result, as $j(\tau) \sim q^{-1}$. □

This refined construction now gives us the following important result.

Corollary. *Singular moduli are algebraic* **integers**.

Proof. Being an algebraic integer means that its a root of an integer polynomial which is also monic. We just showed that $\Psi_m(X, X)$ is monic. □

Example. *Let's look at the factorization of* $\Psi_2(X, X)$ *in more detail. Above, we found that*

$$\Psi_2(X, X) = -(X - 8000)(X + 3375)^2(X - 1728).$$

Consider the three CM points

$$i, \quad \frac{1 + i\sqrt{7}}{2}, \quad i\sqrt{2}.$$

These are fixed by

$$S, \quad \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 2 & 0 \end{pmatrix}$$

respectively, which have determinants 1, 2, *and* 2. *The corresponding singular moduli*

$$j(i) = 1728, \quad j\left(\frac{1 + i\sqrt{7}}{2}\right) = -3375, \quad j(i\sqrt{2}) = 8000$$

are the roots of $\Psi_2(X, X)$.

Example. *More generally, given a discriminant* $D < 0$ *(henceforth, a discriminant is simply an integer congruent to* 0 *or* 1 *modulo* 4*), we can consider the CM point*

$$\tau_D := \begin{cases} \frac{1}{2}\sqrt{D} & \text{if } D \text{ is even,} \\ \frac{1+\sqrt{D}}{2} & \text{if } D \text{ is odd.} \end{cases}$$

Then a few sample values are:

$$j(\tau_{-4}) = 1728, \ j(\tau_{-11}) = -32768.$$

But these are not always integers in $\mathbb{Z}$. *For example,*

$$j(\tau_{-15}) = \frac{-191025 + 85995\sqrt{5}}{2}.$$

6. Connection with quadratic forms

We considered the set of quadratic forms of a given discriminant before, for example when studying the Shimura/Shintani correspondence. Here, we'll set $\mathcal{Q}_D^{\text{prim}}$ to be the set of primitive (has coprime coeffiicents) integral binary quadratic forms $AX^2+BXY+CY^2$ of discriminant $B^2-4AC=D$. If D is a negative discriminant and $Q \in \mathcal{Q}_D^{\text{prim}}$, the **associated CM point**, denoted τ_Q, is the unique root of $Q(\tau,1)$ in $\mathbb{H}$.

There is thus a bijection $\mathcal{Q}_D^{\text{prim}} \leftrightarrow \mathfrak{Z}_D$ with the set of CM points of discriminant D. We've discussed that $\Gamma(1)$ acts on $\mathcal{Q}_D$ (the same is true if we modify our earlier discussion for primitive forms), and the **class number** $h(D)$ is

$$h(D) := \#\Gamma(1)\backslash\mathcal{Q}_D = \#\Gamma(1)\backslash\mathfrak{Z}_D.$$

A set of representative of $\Gamma(1)\backslash\mathcal{Q}_D$ is in fact given by the classical set of **reduced quadratic forms**

$$\mathcal{Q}_D^{\text{red}} := \left\{ [A,B,C] \in \mathcal{Q}_D^{\text{prim}} \;\middle|\; -A < B \leq A < C \;\text{ or } 0 \leq B \leq A = C \right\}.$$

Remark. *This is a finite set as*

$$C \geq A \geq |B| \implies |D| = 4AC - B^2 \geq 3A^2$$

and once A, B are fixed, so is C.

Thus, the class number is finite (in algebraic number theory, recall that this is some measure of how far the set of algebraic integers in $Q(\sqrt{D})$ is from being a UFD; this fact is much harder to prove in general, but is easier thanks to this classical approach Gauss used in the imaginary quadratic field case).

Finally, we let

$$\{\mathfrak{z}_{D,j}\}_{1\leq j\leq h(D)}$$

be a set of representatives for $\Gamma(1)\backslash\mathfrak{Z}_D$. You can do this by picking roots of reduced quadratic forms in $\mathbb{H}$; in fact, an alternative definition of reduced which is where the strange inequalities come from is that the associated CM point is in the fundamental domain $\mathfrak{F}$. We also choose $\mathfrak{z}_{D,1} = \mathfrak{z}_D$, the choice of CM point in the example above.

7. Class Polynomials

We begin this section with an important definition.

Definition. The **class polynomial** of a negative discriminant D is

$$H_D(X) := \prod_{\tau\in\Gamma(1)\backslash\mathfrak{Z}_D} (X - j(\tau)).$$

Theorem. *For any negative discriminant D, we have*

$$H_D(X) \in \mathbb{Z}[X]$$

and that $H_D(X)$ is irreducible.

Corollary. *The singular modulus $j(\tau_D)$ is algebraic of degree the class number $h(D)$ over $\mathbb{Q}$, and its Galois conjugates are the other singular moduli $j(\mathfrak{z}_{D,j})$ (the first part is just due to the fact that H_D is irreducible of degree $h(D)$, the second is a basic consequence of Galois theory, which if you haven't seen, you can ignore).*

Sketch of proof. Before starting, we note that the determinants m above are closely related to the discriminant here, and the feature of the construction of Ψ_m above was that it was uniform in this parameter and didn't depend on the choice of a CM point.

If $\tau \in \mathfrak{Z}_D$, say that its the root of the quadratic equation

$$A\tau^2 + B\tau + C = 0, \quad A > 0$$

and that $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has determinant m and fixes τ. Thus,

$$\frac{a\tau + b}{c\tau + d} = \tau \implies a\tau + b = c\tau^2 + d\tau \implies c\tau^2 + (d-a)\tau - b = 0 \implies (c, d-a, -b) = u(A, B, C)$$

for some $u \in \mathbb{Z}$. Thus,

$$-b = Cu \implies b = -Cu$$

and

$$c = uA,$$

and so

$$M = \begin{pmatrix} a & -Cu \\ Au & d \end{pmatrix}.$$

We also have $d - a = Bu$. Denoting the trace by $t := d + a$, we find that

$$d = \frac{1}{2}(t + Bu), \quad a = \frac{1}{2}(t - Bu).$$

Thus,

$$M = \begin{pmatrix} \frac{1}{2}(t - Bu) & -Cu \\ Au & \frac{1}{2}(t + Bu) \end{pmatrix}$$

$$\implies \det(M) = \frac{1}{4}(t^2 - B^2u^2) + ACu^2 = \frac{1}{4}(t^2 - u^2(B^2 - 4AC)) = \frac{t^2 - Du^2}{4} = m.$$

Conversely, if $t, u \in \mathbb{Z}$ satisfy $t^2 - Du^2 = 4m$, then the equations above give a matrix $M \in \mathcal{M}_m$ fixing τ (that is, all steps are reversible). Thus,

$$\left\{ m \in \mathbb{Z} \;\middle|\; m \text{ is the determinant of a matrix } M \text{ fixing } \tau \right\} = \left\{ \frac{1}{4}(t^2 - Du^2) \text{ where } t \equiv Du \pmod 2 \right\}.$$

In turn, this is the set of **norms** in $\mathbb{Q}(\sqrt{D})$ of elements in $\mathbb{Z}[\mathfrak{z}_D]$ (the norm in $\mathbb{Q}(\sqrt{D})$ of an element $\alpha + \beta\sqrt{D}$ is defined to be $\alpha^2 - D\beta^2$). This shows that the set only depends on D, not on the specific point τ.

We can construct the square of $H_D(X)$ out of gcd's of the polynomials $\Psi_m(X, X)$ above. We first illustrate this in a special case.

Example. *Suppose you want to pick off CM points of discriminant* -7*. We saw above that* $\Psi_2(X,X) = -(X-8000)(X+3375)^2(x-1728)$*. We saw that these three factors were* $j(\tau)$ *for* $\tau = \sqrt{-2}, (1+\sqrt{-7})/2, i$*, respectively. To separate the CM point of discriminant* -7*, we can use matrices of determinant* 3*. One can use the above characterization to check that* $i, \sqrt{-2}$ *are fixed by matrices of determinant* 3*, but that* $(1+\sqrt{-7})/2$ *is not. Then* $\Psi_3(X,X)$ *contains* $X - 1728$ *and* $X - 8000$ *as a factor but not* $X + 3375$*. This allows one to compute that*

$$H_{-7}(X)^2 = (X + 3375)^2.$$

In general, we may pick a prime m_1, the norm of an element of $\mathbb{Z}[\mathfrak{z}_D]$ (it is known that there are infinitely many) and choose finitely many additional m's which are norms of elements of $\mathbb{Z}[\mathfrak{z}_D]$ but not norms in the situations for the (finitely many) other discriminants where m_1 is a norm. We omit the details. This doesn't show that $H_D(X)$ is irreducible, but that can be shown using a more detailed study of CM elliptic curves. □

8. Class number relations

Making this last proof slightly more precise also gives the following result.

Theorem (Kronecker)**.** *We have the factorization*

$$\Psi_m(X,X) = \pm \prod_{D<0} H_D(x)^{\frac{r_D(m)}{w(D)}}, \quad (m \neq \square),$$

where

$$r_D(m) := \#\left\{t, u \;\middle|\; t^2 - Du^2 = 4m\right\}$$

and $w(D)$ *the number of units in* $\mathbb{Z}[\mathfrak{z}_D]$*, explicitly characterized as*

$$w(D) = \begin{cases} 6 & \text{if } D = -3, \\ 4 & \text{if } D = -4, \\ 2 & \text{otherwise.} \end{cases}$$

There is another formulation of this. Let $h^*(D)$ be the number of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of positive definite (this means that at non-zero inputs, the output is always positive), binary integer quadratic forms of discriminant D (not only the primitive ones) counted *with multiplicity* 2 over the order of the stabilizer in $\mathrm{SL}_2(\mathbb{Z})$ (overall, this multiplicity is $1/2, 1/3$ if the corresponding root in $\mathbb{H}$ is equivalent to i, ω, respectively, and one otherwise). Alternatively, we have

$$h^*(D) = \sum_{r^2 | D} h'(D/r^2),$$

where

$$h'(D) := \frac{h(D)}{\frac{1}{2}w(D)}.$$

The corresponding class polynomial is

$$H_D^*(X) = \prod_{r^2|D} H_D(X)^{\frac{2}{w(D)}}$$

(there are only actually fractional powers here if $|D|$ or $3|D|$ is a square).

These give a nicer formula to decompose Ψ_m as

$$\Psi_m(X, X) = \pm \prod_{t^2<4m} H^*_{t^2-4m}(X), \quad (m \neq \square).$$

Comparing degrees gives a very famous result.

Theorem (Hurwitz-Kronecker class number relation)**.** *We have, for m non-square, that*

$$\sigma_1^+(m) = \sum_{D<0} \frac{h(D)}{w(D)} r_D(m) = \sum_{t^2<4m} h^*(t^2 - 4m).$$

Besides being a pretty formula, this gives a way to recursively **compute class numbers**. It turns out that this gives formulas for $h^*(-4m)$ in terms of $h^*(D)$ with $|D| < 4m$, but only half of the discriminants are multiples of 4. However, one can prove another class number relation:

$$\sum_{t^2<4m} (m - t^2) h^*(t^2 - 4m) = \sum_{d|m} (d, m/d)^3.$$

Together, these two class number relations give a recursive way to compute class numbers. These class number relations are also quite deep, for example related to the **Eichler-Selberg trace formulas**, which give the trace of Hecke operators acting on the vector space of cusp forms, and is a basic example of much more general deep results like the Arthur-Selberg trace formula.

9. Crazy numbers, and explicit class field theory

At the beginning of this semester, we talked about how

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999925\ldots$$

is **almost an integer**. We can finally see why. From the above, if $h(D) = 1$, then $j(\mathfrak{z}_D)$ is an algebraic integer inside a degree 1 extension of $\mathbb{Q}$, which is to say, $j(\mathfrak{z}_D) \in \mathbb{Z}$. The most impressive example will come from the largest possible such D (in absolute value). A famous result of Heegner and Stark, which solved an old conjecture of Gauss, states that the largest negative discriminant of class number 1 is $D = -163$. Thus,

$$j\left(\frac{1 + \sqrt{-163}}{2}\right) \in \mathbb{Z}.$$

Since 163 is big, for $\tau = \mathfrak{z}_{163}$,

$$|q| = e^{-\pi\sqrt{163}} \approx 3.8 \cdot 10^{-18}.$$

This is very tiny! Conversely, q^{-1} is huge. So

$$\mathbb{Z} \ni j(\tau) = q^{-1} + 744 + 196884q + O(q^2) \approx q^{-1} + 744.$$

Thus,

$$q^{-1} = -e^{\pi\sqrt{163}} \approx j(\tau) - 744 \in \mathbb{Z}.$$

Finally, we conclude with a very famous application of CM theory. The **Kronecker-Weber** theorem famously answers the question of what number fields are abelian (meaning they have abelian Galois group over $\mathbb{Q}$). Specifically, they are just the subfields of cyclotomic fields $\mathbb{Q}(\zeta_m)$. **Kronecker's Jugendtraum** (dream of youth), also listed as **Hilbert's 12-th problem**, asks if one can do something similar with base field a number field. That is, abelian extensions of $\mathbb{Q}$ are all contained in the fields you get by adjoining roots of unity to $\mathbb{Q}$. These are values of a single transcendental function: the exponential function. The theory of CM we've seen above can be used to show that there is a transcendental function $j(\tau)$, such that when you plug in values, the singular moduli, and adjoin them to imaginary quadratic fields, you find all the abelian extensions of the imaginary quadratic field you started with. These constructions are done using the class polynomials $H_D(X)$ we constructed above. Shimura extended these results to CM number fields; however, the general problem of Hilbert remains open today.