SINGULAR MODULI

SARTH CHAVAN

ABSTRACT. In this survey article, we study singular moduli and its applications.

1. INTRODUCTION

Let $j(z)$ be the classical modular function for $\mathrm{SL}_2(\mathbb{Z})$ defined by

$$\begin{aligned} j(z) &:= \frac{1}{q\prod_{n=1}^{\infty}(1-q^n)^{24}}\left(1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)^3 \\ &= q^{-1}+744+196884q+21493760q^2+\ldots, \end{aligned}$$

where $q=e^{2\pi\imath z}$ and $\sigma_a(n)=\sum_{k|n}k^a$. *Singular moduli* is the classical name for the values assumed by $j(z)$ at imaginary quadratic arguments in the upper half of the complex plane.

Singular moduli are algebraic integers which play prominent roles in classical and modern number theory [1]. For example, Hilbert class fields of imaginary quadratic fields are generated by singular moduli. Furthermore, isomorphism classes of elliptic curves with complex multiplication are also distinguished by singular moduli. These invariants were studied intensively by the leading number theorists since the time of Kronecker and Weber.

Hilbert, in his 9th problem, posed the problem of finding the general reciprocity law for any number field. The class field theory developed in the first half of the 20th century was successful in answering this question for finite abelian extensions of $\mathbb{Q}$.

As an easy consequence of class field theory, one can reproduce the classical Kronecker-Weber theorem, that is, every finite abelian extension of $\mathbb{Q}$ is a subfield of some cyclotomic extension $\mathbb{Q}(\xi_m)$ of $\mathbb{Q}$. Moreover, Hilbert's 12th problem also asked how to extend the Kronecker-Weber theorem to an arbitrary ground number field [1].

Motivated by the case of $\mathbb{Q}$ where all abelian extensions are obtained by adjoining the values of the exponential function, Kronecker conjectured, while he was studying elliptic functions, that all abelian extensions of an imaginary quadratic field should also arise in such a manner. This was achieved by the beautiful theory of complex multiplication, which allows one to describe all abelian extensions of an imaginary quadratic field via the values of the modular j-function and the Weber function, or in the language of elliptic curves, via the j-invariant and (certain powers of) x-coordinates of all torsion points of the corresponding elliptic curve. This problem for general number fields, known as *Kronecker's Jugendtraum* (dream of youth), is still largely open and is at the heart of current research in number theory.

2. Background

2.1. **Elliptic curves and singular moduli.** Let K be a field whose characteristic is not 2 or 3. Then an *elliptic curve* E/K is a nonsingular curve in the projective plane $\mathbb{P}^2$ of the form

$$y^2 = 4x^3 - -\mathfrak{g}_2 x - \mathfrak{g}_3,$$

with $\mathfrak{g}_2, \mathfrak{g}_3 \in K$, whose only point on the line at infinity is $O = [0, 1, 0]$.

The *j-invariant* of an elliptic curve E is defined as the quantity

$$j(E) = \frac{1728\mathfrak{g}_2^3}{\mathfrak{g}_2^3 - 27\mathfrak{g}_3^2},$$

where

$$\mathfrak{g}_2 = 60 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \frac{1}{(m\tau+n)^4}, \quad \mathfrak{g}_3 = 140 \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \frac{1}{(m\tau+n)^6},$$

are multiples of the standard Eisenstein series on the upper half-plane $\mathbb{H}$.

The j-invariant of E uniquely determines its geometric isomorphism class: for elliptic curves E_1/F and E_2/F we have $j(E_1) = j(E_2)$ if and only if E_1 and E_2 are isomorphic over an algebraic closure of F. Such an isomorphism is necessarily defined over a finite extension of F, and for j-invariants other than 0 and 1728 this extension is at most a quadratic extension: if E_1 and E_2 are not isomorphic over F then they are isomorphic over some quadratic field $\mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ squarefree, and if E_1 is defined by $y^2 = x^3 + Ax + B$ then $y^2 = x^3 + d^2 + d^3B$ is a defining equation for E_2 and we say that E_2 is the quadratic twist of E_1 by d. Elliptic curves E over $\mathbb{C}$ are isomorphic (both as elliptic curves and as complex analytic varieties) to $\mathbb{C}/L$ for some lattice L in $\mathbb{C}$. If L has $\mathbb{Z}$-basis ω_1, ω_2 with $\tau = \omega_1/\omega_2$ in the complex upper half-plane, then we set $j(L) = j(\tau)$, the value of the classical elliptic j-function at τ, and we have $j(E) = j(L)$. This value is independent of the (oriented) $\mathbb{Z}$-basis, and homothetic lattices have the same j-invariant. See [16, 18, 19, 22] for more details.

2.2. **Basic CM facts.** An *imaginary quadratic order* is a finite index subring of the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K. Imaginary quadratic orders are in 1-to-1 correspondence with the set of *imaginary quadratic discriminants*: negative integers D that are squares modulo 4. Every such D arises as the discriminant of a unique imaginary quadratic order $\mathcal{O}_D$, and can be written as $D = f^2 D_0$ where the *fundamental discriminant* D_0 is equal to the discriminant D_K of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D_K})$ and $f := [\mathcal{O}_K : \mathcal{O}_D] = \sqrt{D/D_K}$ is the *conductor* of $\mathcal{O}_D$. The class number $h(D) := h(\mathcal{O}_D)$ is the order of the *class group* Cl_D of invertible fractional $\mathcal{O}_D$-ideals modulo principal fractional $\mathcal{O}_D$-deals. The class numbers $h(D)$ are related by the formula [19, Thm. 7.24]

$$h(D) = h(\mathcal{O}_D) = \frac{h(\mathcal{O}_K) f}{[\mathcal{O}_K^\times : \mathcal{O}_D^\times]} \prod_{p \mid f} \left(1 - \left(\frac{D_K}{p}\right)\frac{1}{p}\right), \tag{2.1}$$

where $[\mathcal{O}_K^\times : \mathcal{O}_D^\times]$ is 2 (resp. 3) when $D_K = -4$ (resp. $D_K = -3$) and $f > 1$, and 1 otherwise, and $\left(\frac{D_K}{p}\right) \in \{0, \pm 1\}$ is a Kronecker symbol; the integer $h(\mathcal{O}_K)$ divides $h(D)$.

Fix an embedding of K in $\mathbb{C}$. The image of each invertible $\mathcal{O}_D$-ideal $\mathfrak{a}$ under this embedding is a lattice in $\mathbb{C}$ homothetic to $\mathbb{Z} + \tau\mathbb{Z}$ for some $\tau \in K \subseteq \mathbb{C}$ that we may assume

lies in the upper half plane. We define $j(\mathfrak{a})$ to be the j-invariant of this lattice; such values $j(\mathfrak{a})$ are traditionally called *singular moduli*. Homothetic lattices have the same j-invariant, so $j(\mathfrak{a})$ depends only on the ideal class $[\mathfrak{a}]$ of $\mathfrak{a}$ in Cl_D and may be written as $j([\mathfrak{a}])$. If E is an elliptic curve defined over a number field F with $\mathrm{End}(E)$ an order in the imaginary quadratic field K, then for every prime $\mathfrak{p}$ of F at which E has good reduction, lying above the rational prime p, the reduction is ordinary if $\mathfrak{p}$ splits in K and supersingular if $\mathfrak{p}$ is inert in K. Moreover, in the ordinary case, the reduced curve $\overline{E}$ has the same endomorphism ring $\mathrm{End}(E)$. (See [22, Theorem 13.12].) Let E be an elliptic curve defined over a number field. The (geometric) endomorphism ring $\mathrm{End}(E)$ is an arithmetic invariant that plays a key role in many theorems and conjectures, including those related to the distribution of Frobenius traces such as the Sato–Tate and Lang–Trotter conjectures, and those related to Galois representations associated to E, such as Serre's uniformity question. It is known that the ring $\mathrm{End}(E)$ is isomorphic either to $\mathbb{Z}$, or to an order $\mathcal{O}$ in an imaginary quadratic field, and in the latter case one says that E has complex multiplication (CM). We refer the reader to [19], and also to [20, Ch. II] for CM by the maximal order of an imaginary quadratic field, and to [21, Ch. 6] for the general case.

3. Integrality of the Singular Moduli

Proposition 3.1. *For any proper fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ and $\sigma \in \mathrm{Gal}(H/K)$, we have*

$$j(\mathfrak{p}\mathfrak{a})^{\sigma} = j(\mathfrak{a})$$

for any proper ideal $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}$, where $\mathfrak{q}$ is a prime of K whose Artin symbol is σ. In particular, $\{j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_h)\}$ is the Galois orbit of $j(\mathfrak{a})$ for any proper fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ and $[\mathbb{Q}(j(\mathfrak{a})) : \mathbb{Q}] = [K(j(\mathfrak{a})) : K] = h$, where $h = h(\mathcal{O})$.

Proof. By Chebotarev's density theorem, there are infinite many degree 1 primes $\mathfrak{q}$ of K whose Artin symbol is σ. For all but finitely many such primes $\mathfrak{q}$, we have

$$j(\mathfrak{p}\mathfrak{a})^{\sigma} \equiv j(\mathfrak{p}\mathfrak{a})^{p} \equiv j(\mathfrak{a}) \,(\mathrm{mod}\, \mathfrak{P}),$$

where $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}$ is proper and $\mathfrak{P}$ is any prime of H over p. Since these $\mathfrak{p}$'s have the same Artin symbol, they must lie in the same ideal class of $\mathcal{O}$. So $j(\mathfrak{p}\mathfrak{a})^{\sigma} - j(\mathfrak{a})$ is the same for every $\mathfrak{p}$ and has infinitely many prime factors, therefore it must be zero. We conclude that $j(\mathfrak{p}\mathfrak{a})^{\sigma} = j(\mathfrak{a})$. The remaining part follows since $[K : \mathbb{Q}] \leqslant 2$ and $[\mathbb{Q}(j(\mathfrak{a})) : \mathbb{Q}] \leqslant h$. ∎

We have seen that $j(\mathfrak{a})$ is an algebraic number of degree $h(\mathcal{O})$ from the above Theorem. However, it turns out that it is also an algebraic integer. This is always the case, and the goal of this section is to explain this phenomenon. There are three possible proofs of this fact: the complex analytic proof using the modular equation, the l-adic good reduction argument proof due to Serre and Tate [10], and the p-adic bad reduction argument proof, again due to Serre [12, II.6]. For convenience, we will choose the first approach here, as the other two arguments go beyond the scope of this paper.

Let us first recall some facts about the modular curve $X_0(N)$, which plays an important role in modern number theory. The modular curve $X_0(N)$ is a compact Riemann surface constructed by compactifying $\Gamma_0(N)\backslash\mathcal{H}$, the quotient of upper half plane by the congruence group $\Gamma_0(N)$. It is the compactification of the moduli space of elliptic curves along with the level structure of a cyclic subgroup of order N.

Viewing $X_0(N)$ as a complex algebraic curve, the function field of $X_0(N)$ is equal to $\mathbb{C}(j(N\tau), j(\tau))$. So $X_0(N)$ has a planar model defined by say some complex polynomial $\Phi_N(X, Y)$ satisfying $\Phi_N(j(N\tau), j(\tau)) = 0$, called the modular equation of level N.

An unexpected result is that the modular equation $\Phi_N(X, Y)$ in fact has rational, or even better, integer coefficients. Therefore, $X_0(N)$ can be defined as an algebraic curve over $\mathbb{Q}$ without reference to the complex numbers and it has a planar model over $\mathbb{Q}$ defined by the modular equation. The goal of this section is to prove this unexpected fact and deduce the integrality of $j(\mathfrak{a})$ as a consequence. See [1] for more rigorous details. However, to define the modular equation, we need the following important proposition.

Proposition 3.2 (Hasse q-expansion principle)**.** *Let $f(\tau)$ be a modular function with respect to $\Gamma(1)$ with the q-expansion $\sum_{n=-t}^{\infty} c_n q^n$. Then f can be expressed as a polynomial of degree t in $\mathbb{Z}[c_{-t}, \ldots, c_0][j(\tau)]$. In particular, if $c_i \in \mathbb{Z}$, then this polynomial has integer coefficients.*

Proof. The proof is by induction on t. When $t = 0$, $f(\tau)$ is a holomorphic function on the compact Riemann surface $X(1)$, hence it must be the constant c_0. When $t > 0$, since $j(\tau)$ has q-expansion $\frac{1}{q} + 744 + \cdots$ with integer coefficients, the leading term of the q-expansion of $f - c_{-t}j^t$ is $(c_{1-t} - 744)q^{1-t}$ and all the coefficients are in $\mathbb{Z}[c_{1-t}, \ldots, c_0]$. Now applying the induction hypothesis, we know $f - c_{-t}j^t \in \mathbb{Z}[c_{1-t}, \ldots, c_0][j]$ is a polynomial of degree $t - 1$, which produces the desired result. ∎

Definition 3.3. Let

$$\Delta_N = \left\{ A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} : \det(A) = N, \gcd(a, b, c, d) = 1 \right\}.$$

Suppose $\{\gamma_i\}$ is a set of orbit representatives for the left action of $\Gamma(1)$ on Δ_N. We define

$$\Phi_N(X, j(\tau)) = \prod_i (X - j(\gamma_i \tau)).$$

Then the coefficients of X in $\Phi_N(X, j(\tau))$ are modular functions of $\Gamma(1)$, hence by Lemma 3, these coefficients of X are polynomials in $j(\tau)$. So $\Phi_N(X, Y)$ is a polynomial, called the *modular polynomial* or the *modular equation* of level N.

Since $\begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix} \in \Delta_N$, it follows immediately that $\Phi_N(j(N\tau), j(\tau)) = 0$. Also, it is an easy computation to see that the set of orbit representatives can be chosen as

$$C(N) = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : ad = N, a > 0, 0 \leqslant b < d, \gcd(a, b, d) = 1 \right\}.$$

Theorem 3.4. *The modular equation $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$. Moreover, when N is not a perfect square, the leading coefficient of $\Phi_N(X, X)$ is ± 1.*

Proof. By Proposition 3.2, to show $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$, it suffices to show that the q-expansions of $\Phi_N(X, j(\tau))$ have integer coefficients. Using the orbit representatives in $C(N)$, we find that for $\gamma_i = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, $j(\gamma_i \tau)$ has a Fourier expansion in $q^{a/d}$ with coefficients in $\mathbb{Z}[\xi]$ where $\xi = e^{2\pi i/N}$, hence the coefficients of q-expansions of $\Phi_N(X, j(\tau))$ are

in $\mathbb{Z}[\xi]$. For an integer r prime to N, the map

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mapsto \begin{bmatrix} a & br \mod d \\ 0 & d \end{bmatrix}$$

is a permutation of $C(N)$, hence it leaves $\Phi_N(X, j(\tau))$ unchanged. But this map has an action $\xi \mapsto \xi^r$ on the coefficients, therefore the coefficients are actually in $\mathbb{Z}$. So $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$. Now suppose N is not a perfect square.

The leading coefficient of $\Phi_N(X, X)$ is the same as the leading coefficient of the q-expansion of $\Phi_N(j(\tau), j(\tau))$, so let us show that the latter is ± 1. Now $j(\tau)$ begins with q^{-1} and $j(\gamma_i\tau)$ begins with $\xi^d q^{-a/d}$, so since N is not a perfect square and $ad = N$, we know that q^{-1} and $\xi^d q^{-a/d}$ cannot cancel out, hence the leading coefficient of $j(\tau) - j(\gamma_i\tau)$ is a root of unity. Multiplying them together, we know that the leading coefficient of $\Phi_N(j(\tau), j(\tau))$ is a root of unity. But we already know it is an integer, hence it must be ± 1. ∎

Example 3.5. The first two modular equations are computed as

$$\begin{aligned} \Phi_1(X, Y) &= X - Y, \\ \Phi_2(X, Y) &= X^3 + Y^3 - X^2Y^2 + 2^4 \cdot 3 \cdot 31(X^2Y + Y^2X) - 2^4 \cdot 3^4 \cdot 5^3(X^2 + Y^2) \\ &\quad + 3^4 \cdot 5^3 \cdot 4027XY + 2^8 \cdot 3^7 \cdot 5^6(X + Y) - 2^{12} \cdot 3^8 \cdot 5^9. \end{aligned}$$

Now we are in a position to prove the integrality of the singular moduli.

Theorem 3.6. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K and $\mathfrak{a}$ be a proper fractional ideal of $\mathcal{O}$. Then $j(\mathfrak{a})$ is an algebraic integer of degree $h(\mathcal{O})$.*

Proof. By Chebotarev's density theorem, there are infinitely many degree 1 primes of $\mathcal{O}$ in the principal ideal class. Let $\mathfrak{p}$ be such a prime. Then $\mathfrak{a}/\mathfrak{p}\mathfrak{a} \cong \mathbb{Z}/p\mathbb{Z}$ where $p = N(\mathfrak{p})$ is a prime. We may assume that $\mathfrak{a} = \mathbb{Z} + \mathbb{Z}\tau$, then $\mathfrak{p}\mathfrak{a}$ is homothetic to $\mathbb{Z} + \mathbb{Z}\gamma\tau$ for some $\gamma \in \Delta_p$ ([3, 11.24]). We know that $\Phi_p(j(\mathfrak{a}), j(\mathfrak{p}\mathfrak{a})) = 0$ by definition. But $j(\mathfrak{p}\mathfrak{a}) = j(\mathfrak{a})$ by our choice of $\mathfrak{p}$. Hence by Theorem 7, $j(\mathfrak{a})$ satisfies the polynomial $\Phi_p(X, X) \in \mathbb{Z}[X]$ with leading coefficient ± 1 and therefore $j(\mathfrak{a})$ is an algebraic integer. ∎

4. Gross-Zagier's Theorem on Singular Moduli

Gross and Zagier [16] proved a result which completely determines the prime factorization of the norm of the difference between two singular moduli, which in turn justified many classical conjectures on the congruences of singular moduli proposed by Berwick [4]. They provide two proofs of different natures: The first proof, an algebraic proof, is based on Deuring's work on endomorphism rings of elliptic curves. The second analytic proof relies on the calculation of the Fourier coefficients of the restriction to the diagonal $\mathcal{H} \subseteq \mathcal{H} \times \mathcal{H}$ of an Eisenstein series of the Hilbert modular group of $\mathbb{Q}(\sqrt{D})$. As the authors remarked, these two methods can be viewed as the special case $N = 1$ of the theory of local heights of Heegner points on $X_0(N)$, which generalizes to groundbreaking Gross-Zagier formula [17].

In this section (which is reproduced from [1]), we will first state the famous Gross-Zagier's theorem, then use it to compute several examples and derive some consequences.

Now consider two orders with discriminants d_1 and d_2 satisfying $\gcd(d_1, d_2) = 1$. Let w_1, w_2 be the numbers of their units and h_1, h_2 be their class numbers. Let $\mathfrak{a}_i$ $(1 \leqslant i \leqslant h_1)$

and $\mathfrak{b}_k$ $(1 \leqslant k \leqslant h_2)$ be the representatives of their ideal class groups. Define

$$J(d_1, d_2) = \left(\prod_{i=1}^{h_1} \prod_{k=1}^{h_2} (j(\mathfrak{a}_i) - j(\mathfrak{b}_k)) \right)^{4/w_1 w_2}.$$

Notice that when $w_1 w_2 = 4$ (e.g., $d_1, d_2 < -4$), $J(d_1, d_2)$ is just the norm of any of the differences $j(\mathfrak{a}_i) - j(\mathfrak{b}_k)$. In general, $J(d_1, d_2)$ is a certain power of this norm and $J(d_1, d_2)^2$ is always an integer. To state Gross-Zagier's theorem, let us introduce some notation. Let $D = d_1 d_2$. For a prime p, define

$$\epsilon(p) = \begin{cases} \left(\dfrac{d_1}{p}\right), & p \nmid d_1, \\ \left(\dfrac{d_2}{p}\right), & p \nmid d_2. \end{cases}$$

This is well-defined whenever $\left(\frac{D}{p}\right) \neq -1$. More generally, if n has the prime factorization $n = \prod_{i=1}^{r} p_i^{a_i}$ with $\left(\frac{D}{p_i}\right) \neq -1$, we define

$$\epsilon(n) = \prod_{i=1}^{r} \epsilon(p_i)^{a_i}.$$

Finally, set

$$F(m) = \prod_{\substack{nn'=m, \\ n,n'>0}} n^{\epsilon(n')}.$$

This is well-defined whenever all primes p dividing m satisfy $\left(\frac{D}{p}\right) \neq -1$. Now we are finally ready to state our main theorem, which is as follows.

Theorem 4.1 (Gross-Zagier Theorem [16])**.** *With the above notation,*

$$J(d_1, d_2)^2 = \pm \prod_{\substack{x^2 < d_1 d_2 \\ x^2 \equiv d_1 d_2 \pmod 4}} F\left(\frac{d_1 d_2 - x^2}{4}\right).$$

Example 4.2. When $d_1 = -3$, we know the corresponding $w_1 = 6$ and $j\left(\frac{1+\sqrt{-3}}{2}\right) = 0$. So in this case,

$$J(-3, d_2) = N\left(j\left(\frac{d_2 + \sqrt{d_2}}{2} \right) \right)^{2/(3w_2)}.$$

In particular, for $d_2 = -163$, $w_2 = 1$ and $h_2 = 1$, so we have $j\left(\frac{1+\sqrt{-163}}{2}\right) = J(-3, -163)^3$. The factors of $J(-3, -163)^2$ are tabulated in an online database, so we can conclude that

$$j\left(\frac{1+\sqrt{-163}}{2}\right) = -(2^6 \cdot 3 \cdot 5 \cdot 23 \cdot 29)^3.$$

Finally, let us come to the algebraic proof of Gross-Zagier's theorem. The proof proceeds locally. As the first step, Gross and Zagier relate the valuation of the difference of two j-values to the geometry of elliptic curves and reduce it to a counting problem of isomorphisms between elliptic curves. Next, a generalization of Deuring's lifting theorem will allow one to reduce the problem to counting certain subrings of the endomorphism ring of a supersingular elliptic curve. To complete the proof, Gross and Zagier give a convenient description of a maximal order and its subrings in the rational quaternion algebra ramified at ∞ and a prime for explicit computation. The first step can be viewed as an interesting geometrical interpretation of the difference of j-values.

Proposition 4.3. *Let W be a complete discrete valuation ring whose quotient field has characteristic zero and whose residue field is algebraically closed and has characteristic $\ell > 0$ (e.g., $W(\overline{\mathbb{F}_\ell})$). Let π be its uniformizer and v be its normalized valuation. Let E, E' be elliptic curves defined over W with good reduction and j-invariants j, j'. Denote the set of isomorphisms from E to E' defined over W/π^n by $\mathit{Iso}_n(E, E')$. Then*

$$v(j - j') = \frac{1}{2} \sum_{n \geq 1} \#\mathit{Iso}_n(E, E').$$

Proof. We may assume that E, E' are isomorphic over the algebraically closed field W/π, otherwise both sides are zero. Denote $i(n) = \frac{1}{2}\#\mathrm{Iso}_n(E, E')$, then $i(1) \geqslant 1$. Let us consider the case when $\ell \neq 2, 3$ for simplicity. Change models for E, E' with simplified Weierstrass equations

$$y^2 = x^3 + a_4 x + a_6, \quad y^2 = x^3 + a_4' x + a_6'.$$

By definition, we have $i(n) \geqslant 1$ if and only if we can solve the congruences

$$\begin{cases} a_4 \equiv u^4 a_4' \\ a_6 \equiv u^6 a_6' \end{cases} (\mathrm{mod}\, \pi^n)$$

simultaneously for some unit $u \in (W/\pi^n)^*$. In this case $\Delta = -16(4a_4^3 + 27a_6^2)$, and at least one of a_4 and a_6 is a unit in W^* since E has good reduction mod π.

If a_4 is a unit in W^*, then a_4' is also a unit. By changing models we may assume that $a_4 = a_4' = 1$. Then

$$v(j - j') = v(a_6^2 - a_6'^2) = v(a_6 - a_6') + v(a_6 + a_6').$$

On the other hand, the congruences become

$$\begin{cases} u^4 \equiv 1 \\ a_6 \equiv u^6 a_6' \end{cases} (\mathrm{mod}\, \pi^n)\ .$$

We may possibly modify (a_6, a_6') by ± 1 so that $v(a_6 - a_6')$ is maximal. Then

$$i(n) = \begin{cases} 0\ (\text{no solution}), & n > v(a_6 - a_6'), \\ 1\ (u = \pm 1), & v(a_6 + a_6') < n \leqslant v(a_6 - a_6'), \\ 2\ (u = \pm 1, \pm i), & n \leqslant v(a_6 + a_6'). \end{cases}$$

We get

$$\sum_{n\geqslant 1} i(n) = v(a_6 - a_6') + v(a_6 + a_6').$$

So the theorem holds in this case.

If a_6 is a unit in W^*, then a_6' is also a unit. Similarly by changing models we may assume that $a_6 = a_6' = 1$. Then

$$\begin{aligned} v(j - j') &= v(a_4^3 - a_4'^3) = v(a_4 - a_4') + v(a_4 - \rho a_4') + v(a_4 - \rho^2 a_4') \\ &= v(a_4 - a_4') + 2v(a_4 - \rho a_4'), \end{aligned}$$

where ρ is a primitive cube root of unity in W^*. On the other hand, the congruences become

$$\begin{cases} a_4 \equiv u^4 a_4' \\ u^6 \equiv 1 \end{cases} (\mathrm{mod}\, \pi^n)\ .$$

We may possibly modify (a_4, a_4') by ρ or ρ^2 so that $v(a_4 - a_4')$ is maximal. Then

$$i(n) = \begin{cases} 0\ (\text{no solution}), & n > v(a_4 - a_4'), \\ 1\ (u = \pm 1), & v(a_4 - \rho a_4') < n \leqslant v(a_4 - a_4'), \\ 3\ (u = \pm 1, \pm\rho, \pm\rho^2), & n \leqslant v(a_4 - \rho a_4'). \end{cases}$$

We get

$$\sum_{n\geqslant 1} i(n) = v(a_4 - a_4') + 2v(a_4 - \rho a_4').$$

This completes the proof. ■

or simplicity, we will assume $d_1 = -p$ is a prime from now on (for the general case, see [11]). Let $\mathcal{O}_K$ be the ring of integers of $K = \mathbb{Q}(\sqrt{-p})$. Let E be an elliptic curve over W with complex multiplication by $\mathcal{O}_K$ and with j-invariant $j = j(\mathcal{O}_K)$. For our purpose, we need to calculate $\#\mathrm{Iso}_n(E, E')$ where E' is an elliptic curve over W with complex multiplication by some ring $\mathbb{Z}[w]$ of discriminant d_2. We can rewrite $\#\mathrm{Iso}_n(E, E')$ in a manner which only depends on E. Suppose $f \in \mathrm{Iso}_n(E, E')$, then $w_f = f^{-1} \circ w \circ f \in \mathrm{End}_n(E)$ is an endomorphism of E mod π^n, which has the same norm, trace and action on tangent space as w. Namely, w_f belongs to the set

$$S_n = \{\alpha_0 \in \mathrm{End}_n(E) \mid \mathrm{T}(\alpha_0) = \mathrm{T}(w), \mathrm{N}(\alpha_0) = \mathrm{N}(w), \alpha_0 = w \text{ on } \mathrm{Lie}(E)\},$$

Conversely, every element of S_n is of the form w_f for some unique f ensured by the following lifting theorem, which is a refinement of Deuring's lifting theorem.

Theorem 4.4. *Let E_0 be an elliptic curve over W/π^n and $\alpha_0 \in \mathrm{End}(E_0)$. Assume that $\mathbb{Z}[\alpha_0]$ is a $\mathbb{Z}$-module of rank 2 and is integrally closed in its quotient field. Suppose α_0 induces multiplication by a quadratic element w_0 on $\mathrm{Lie}(E_0)$. If there exists $w \in W$ that*

$$w \equiv w_0\, (\mathrm{mod}\, \pi^n), \qquad w^2 - \mathrm{T}(w_0)w + \mathrm{N}(w_0) = 0,$$

then there exists an elliptic curve E over W and $\alpha \in \mathrm{End}(E)$, such that (E, α) reduces to (E_0, α_0) mod π^n and α induces multiplication by w on $\mathrm{Lie}(E)$.

Now by the above Theorem, we reduce to the counting problem of S_n.

When $\left(\frac{\ell}{p}\right) = 1$, ℓ splits in $K = \mathrm{End}(E) \otimes \mathbb{Q}$, so E has ordinary reduction mod π and $\mathrm{End}_n(E) = \mathrm{End}(E) = \mathcal{O}_K$ ([12, 13.12]). But $\mathcal{O}_K$ contains no elements of discriminant d_2, so S_n is empty for all $n \geq 1$. (Another way to say this: if two elliptic curves E and E' with complex multiplication have the isomorphic reduction $\tilde{E}$, then the reduction $\tilde{E}$ must be supersingular, since two different orders $\mathrm{End}(E)$ and $\mathrm{End}(E')$ have to embed into $\mathrm{End}(\tilde{E})$).

So we only need to consider the case $\left(\frac{\ell}{p}\right) \neq 1$ and E has supersingular reduction. Then $\mathrm{End}_1(E)$ is a maximal order in the rational quaternion algebra B ramified at ℓ and ∞. The algebra B can be desribed explicitly as a subring of $M_2(K)$,

$$B = \left\{ \begin{bmatrix} \alpha & \beta \\ -\ell\bar{\beta} & \bar{\alpha} \end{bmatrix} : \alpha, \beta \in K \right\}.$$

The subrings $\mathrm{End}_n(E)$ can also be desribed explicitly. Using these descriptions, it turns out that in many cases $\#S_n$ equals to $w_1/2$ times the number of the solutions $(x, \mathfrak{b})$ (under certain conditions on $\mathfrak{b}$) of the equation

$$x^2 + 4\ell^{2n-1}\mathrm{N}(\mathfrak{b}) = pq,$$

where we assume $d_2 = -q$ is a prime . The more precise result is the following.

Theorem 4.5. *Let λ be a prime of $\mathcal{O}_K$ over ℓ, then*

$$\mathrm{ord}_\lambda(J(-p,-q)) = \frac{1}{2}\sum_{x\in\mathbb{Z}}\sum_{n\geq 1}\delta(x)R\left(\frac{pq-x^2}{4\ell^n}\right), \tag{2}$$

where

$$\delta(x) = \begin{cases} 2, & x \equiv 0 \,(\mathrm{mod}\, p), \\ 1, & \textit{otherwise}, \end{cases}$$

and $R(m)$ is the number of ideals of $\mathcal{O}_K$ of norm m.

Remark 4.6. The main theorem of Gross and Zagier is now can be derived directly from equation (2) using the formula

$$R(m) = \sum_{n|m, n>0}\left(\frac{n}{p}\right).$$

5. Hilbert Class Polynomials (HCPs)

5.1. **Overview.** Let $E/\mathbb{C}$ be an elliptic curve E over $\mathbb{C}$ that has *complex multiplication* (CM) by an imaginary quadratic order $\mathcal{O}$, by which we mean that the endomorphism ring $\mathrm{End}(E)$ is isomorphic to $\mathcal{O}$. Let K denote the fraction field of $\mathcal{O}$. The j-invariant of E is an algebraic integer whose minimal polynomial over K is the *Hilbert class polynomial* H_n[1], where $-n$ is the discriminant of $\mathcal{O}$.

[1]Note that most authors use the term *Hilbert class polynomial* only when $\mathcal{O}$ is a maximal order (they then use the term *ring class polynomial* for the general case); however, we will not make this distinction.

In particular, the Hilbert class polynomial H_n is defined by

$$H_n(x) := \prod_{j(E)\in \mathrm{Ell}_{\mathcal{O}}(\mathbb{C})} (x - j(E)),$$

where $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C}) := \{j(E/\mathbb{C}) : \mathrm{End}(E) \cong \mathcal{O}\}$ is the set of j-invariants of elliptic curves $E/\mathbb{C}$ with complex multiplication by the order $\mathcal{O}$ with discriminant $-n = \mathrm{disc}(\mathcal{O})$.

Moreover, $H_n \in \mathbb{Z}[x]$ and its splitting field over the imaginary quadratic field K is the *ring class field* $K_{\mathcal{O}}$, which is an abelian extension of K whose Galois group $\mathrm{Gal}\,(K_{\mathcal{O}}/K)$ is isomorphic to the class group $\mathrm{Cl}\,(\mathcal{O})$, via the Artin map. In particular, $\mathrm{Gal}\,(K_{\mathcal{O}}/K)$ is abelian of order $h(D)$. This is indeed a remarkable result as it implies that of uncountably many isomorphism classes of elliptic curves over $\mathbb{C}$, only countably many have CM.

The degree of the Hilbert class polynomial H_D is the class number $h(D)$. For any positive integer h only finitely many negative discriminants D have class number $h(D) = h$. For example, when $h = 1$ there are 13 (of which 9 are fundamental), corresponding to the 13 CM j-invariants that lie in $\mathbb{Q}$. For $h \leqslant 100$ the complete list of discriminants $D < 0$ with $h(D) = h$ is known. All such fundamental discriminants D_0 were enumerated by Watkins [13], and Klaise [15] used this list and the formula for $h(D)$ as a multiple of $h(D_0)$ listed in (1) to determine all negative discriminants D with $h(D) \leqslant 100$. In fact, there are a total of 66,758 such discriminants, of which 42,272 are fundamental.

When D is a fundamental discriminant the ring class field of $\mathcal{O}_D$ is the *Hilbert class field* of K, its maximal unramified abelian extension, and in general the extension $K_{\mathcal{O}}/K$ is ramified only at primes that divide the conductor f of $\mathcal{O}_D$ and must be ramified at all odd primes that do. The extension $K_{\mathcal{O}}/\mathbb{Q}$ is Galois, and unramified at primes not dividing D. To summarize the above discussion, we state the following main theorem.

Theorem 5.1. *Let $\mathcal{O}$ be the maximal order in an imaginary quadratic field of discriminant D, and let L be the splitting field of $H(x)$ over $K = \mathbb{Q}(\sqrt{D})$. The Hilbert class polynomial $H(x)$ is irreducible and has degree equal to the size of the ideal class group, and there is an isomorphism between the ideal class group and the Galois group* $\mathrm{Gal}(L/K)$.

The proofs and necessary background to understand these ideas, as well as some further discussion of topics like the splitting of primes in imaginary quadratic fields and the action of the Galois group $\mathrm{Gal}(L/K)$, can be found in lectures 21–22 of [13] and chapter 6 of [15].

One may ask, whether a given monic, irreducible, integer polynomial H is or is not an Hilbert class polynomial (HCP), and if so, to determine discriminant D for which $H = H_D$. Sutherland and Cremona [18] recently answered these very interesting questions by providing deterministic and probabilistic algorithms. We will see one of them below.

Theorem 5.2. *Given a monic irreducible polynomial $H \in \mathbb{Z}[X]$, Algorithm 1 returns* `true` *and the discriminant D if and only if H is the Hilbert class polynomial H_D.*

Algorithm 1. Given a monic irreducible $H \in \mathbb{Z}[X]$ of degree h, determine if $H = H_D$ for some D. If so, return `true` and the value of D, otherwise return `false`.

Let $\mathcal{D}$ be the set of integers $h^+|h$ that are powers of 2 of the same parity as h.
Let $p_{\min} := \lceil 37h^2(\mathrm{llog}(h+1)+4)^4 \rceil$.
For increasing primes $p \geqslant p_{\min}$:

(1) Compute $\overline{H} := H \bmod p \in \mathbb{F}_p[x]$.
(2) Compute $d := \deg \gcd(\overline{H}(x), x^p - x)$.
(3) If $d = 0$ then proceed to the next prime p.
(4) If $\gcd(\overline{H}, \overline{H}') \neq 1$ then proceed to the next prime p.
(5) If $d < h$ and $d \notin \mathcal{D}$ then return `false`.
(6) Let $\overline{E}/\mathbb{F}_p$ be an elliptic curve whose j-invariant is a root of $\overline{H}$.
(7) If $\overline{E}$ is supersingular then proceed to the next prime p.
(8) Compute $D := \operatorname{disc}(\operatorname{End}(\overline{E})) \in \mathbb{Z}$
(9) If $h(\operatorname{disc} \operatorname{End}(\overline{E})) \neq h$ return `false`, otherwise compute $H_D(X)$.
(10) If $H = H_D$ then return `true` and D; otherwise return `false`.

Moreover, the authors also prove the following important results [18].

Proposition 5.3. *Let D be an imaginary quadratic discriminant and let p be a prime for which $\left(\frac{D}{p}\right) = +1$. Then the Hilbert class polynomial H_D is squarefree modulo p.*

Proposition 5.4. *Let $H(X) \in \mathbb{Z}[X]$ be a polynomial of degree h with exactly h^+ real roots. If H is a Hilbert class polynomial then the following hold:*

(1) *$h^+ \mid h$;*
(2) *h^+ is a power of 2;*
(3) *$h^+ \equiv h \pmod 2$; that is, $h^+ = 1$ if and only if h is odd.*

For example, an HCP of odd degree has exactly one real root, so an odd degree polynomial with any other number of real roots is not an HCP.

5.2. **Ramanujan class polynomials.** This subsection is reproduced from [6].

Let us now turn our attention toward a class of comparatively less studied polynomials that were defined by Ramanujan in the 19th century. Ramanujan, who made many beautiful and elegant discoveries in his short life of 32 years, defined in his third notebook [9, Pages 392-393] the values

$$t_n := \frac{f\left(\sqrt[3]{q_n}\right) f\left(q_n^3\right)}{f^2\left(q_n\right)} \sqrt{3} q_n^{1/18},$$

where $q_n = \exp\left(-\pi\sqrt{n}\right)$, and $f\left(-q\right) = \prod_{n \geqslant 1}\left(1-q^n\right)$.

For all positive $n \equiv 11 \pmod{24}$, let $\mathcal{P}_n$ be the minimal polynomial of t_n over $\mathbb{Q}$. We refer to $\mathcal{P}_n$ a a Ramanujan class polynomial. Without any further explanation on how he found them, Ramanujan gave the following table of polynomials $\mathcal{P}_n$ based on t_n for the first five values of $n \equiv 11 \pmod{24}$: Berndt and Chan [5, Theorem 1.2] later verified his

n	$\mathcal{P}_n(z)$
11	$z - 1$
35	$z^2 + z - 1$
59	$z^3 + 2z - 1$
83	$z^3 + 2z^2 + 2z - 1$
107	$z^3 - 2z^2 + 4z - 1$

Table 1: $\mathcal{P}_n$ for $n = 11, 35, 59, 83, 107$.

claims for $n = 11, 35, 59, 83$, and 107 using laborious computations involving Greenhill polynomials and Weber class invariants, and proved that each $\mathcal{P}_n$ has t_n as a root. However, due to computational complexity, their method to contruct $\mathcal{P}_n$ could not be applied for higher values of n. Thus, they asked for an efficient way of computing the polynomials $\mathcal{P}_n$ for every $n \equiv 11 \pmod{24}$. Moreover, the authors proved the following crucial result [5, Thm. 4.1]:

Theorem 5.5. *Let $n \equiv 11 \pmod{24}$ be squarefree, and suppose that the class number of $\mathbb{Q}(\sqrt{-n})$ is odd. Then t_n is a real unit generating the Hilbert class field of $\mathbb{Q}(\sqrt{-n})$.*

Ten years later, Konstantinou and Kontogeorgis [7] generalized this result by removing the constraint of the class number needing to be odd and also provided an efficient method for constructing the minimal polynomials $\mathcal{P}_n$ of t_n over $\mathbb{Q}$ from the Ramanujan values t_n for $n \equiv 11 \pmod{24}$, using the Shimura reciprocity law, and thus answered the demand made in [5] for a direct and an easily applicable construction method. Moreover, the authors also proved that the t_n is a class invariant for $n \equiv 11 \pmod{24}$ [7, Theorem 3.4].

It is interesting to point out that coefficients of the polynomial $\mathcal{P}_n$ have remarkably smaller size compared to the coefficients of the corresponding Hilbert class polynomial H_n, which is a clear indication that their use in the CM method, which is used for the generation of elliptic curves over prime fields, can be especially favoured. The above discussion also suggests that the polynomials $\mathcal{P}_n$ can be used in the CM method because their roots can be transformed to the roots of H_n. For more details on constructing elliptic curves with CM method, see [2, 3].

The author in [6] studies the discriminants of $\mathcal{P}_n$; the historical precedent for doing so comes from [16], which is known for computing the prime factorization of certain resultants of Hilbert class polynomials. Gross and Zagier [16] also computed the prime factorization of the discriminant of Hilbert class polynomial associated to fundamental discriminant $-p$, where $p \equiv 3 \pmod{4}$ is a prime. This result was later generalized by Dorman [14], who extended the discriminant formula to the Hilbert class polynomials associated with arbitrary fundamental discriminants. Dorman's result in turn was then extended by Ye [23], who computed the prime factorization of HCPs associated to certain non-fundamental discriminants.

In particular the author [6] proved the following results which establish connection between the discriminants of the Hilbert class polynomial H_n and Ramanujan polynomial $\mathcal{P}_n$.

Theorem 5.6. *For all positive $n \equiv 11 \pmod{24}$, we have*

$$\Delta(H_n) = \Delta(\mathcal{P}_n)\left[\mathbb{Z}[t_n] : \mathbb{Z}[\mathrm{j}_n]\right]^2,$$

where $[\mathbb{Z}[t_n] : \mathbb{Z}[\mathrm{j}_n]]$ is the index of $\mathbb{Z}[\mathrm{j}_n]$ in $\mathbb{Z}[t_n]$.

Remark 5.7. Since the quotient $\left[\mathbb{Z}[t_n] : \mathbb{Z}[\mathrm{j}_n]\right]^2$ is a perfect square, we deduce that $\Delta(H_n)$ and $\Delta(\mathcal{P}_n)$ have the same sign for all positive integers $n \equiv 11 \pmod{24}$.

Theorem 5.8. *For all positive $n \equiv 11 \pmod{24}$, $\Delta(\mathcal{P}_n) > 0$ if and only if*

$$h_n \equiv \left|\mathrm{Cl}(n)[2]\right| \pmod{4},$$

where $\mathrm{Cl}(n)[2]$ is the subgroup of $\mathrm{Cl}(n)$ consisting of elements of order at most 2.

Theorem 5.9. *For all positive squarefree integers $n \equiv 11 \pmod{24}$, we have $3 \nmid \Delta(\mathcal{P}_n)$.*

One may ask, whether a given monic, irreducible, integer polynomial P is or is not an Ramanujan class polynomial $\mathcal{P}_n$, and if so, to determine discriminant n for which $P = \mathcal{P}_n$, and see if we can obtain analogues conditions given in Proposition 5.4.

REFERENCES

[1] Chao Li, Endomorphism rings of elliptic curves and singular moduli. Minor thesis.
[2] A. O. L. Atkin and F. Morain, Elliptic curves and primality proving. Math. Comp. **61** (1993), 203, 29–68.
[3] Reinier Bröker and Peter Stevenhagen, Efficient CM-constructions of elliptic curves over finite fields, Mathematics of Computation **76** (2007), 2161–2179.
[4] Berwick, W. E. H, Modular Invariants Expressible in Terms of Quadratic and Cubic Irrationalities, Proc. London Math. Soc. 28 (1927), 53-69.
[5] B. C. Berndt and H. H. Chan, Ramanujan and the modular j-invariant. Canad. Math. Bull. **42**, 4, 427-440.
[6] S. Chavan. On discriminants of minimal polynomials of the Ramanujan t_n class invariants. Bulletin of the Australian Mathematical Society, 1–12, 2023.
[7] E. Konstantinou, A. Kontogeorgis, Computing Polynomials of the Ramanujan t_n Class Invariants, Canad. Math. Bull. Vol. **52** (4), 2009.
[8] Georg-Johann Lay and Horst G. Zimmer, Constructing elliptic curves with given group order over large finite fields, Algorithmic Number Theory Symposium–ANTS I (L. M. Adleman and M.D. Huang, eds.), Lecture Notes in Computer Science, **877**, 1994, pp. 250–263.
[9] S. Ramanujan, Notebooks. Vols. 1, 2, TIFR, Bombay, 1957.
[10] Serre, J.P. & Tate, J., Good reduction of abelian varieties, *Ann. Math.* **88** (1968), 492–517.
[11] Silverman, J. *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.
[12] Silverman, J. *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York, 1994.
[13] A. Sutherland. 18.783 Lectures – Elliptic Curves, 2019.
[14] Dorman, D.R. Singular moduli, modular polynomials, and the index of the closure of $\mathbb{Z}[j(\tau)]$ in $\mathbb{Q}(j(\tau))$. Math. Ann. **283**, 177–191 (1989).
[15] D. Zagier. Elliptic Modular Forms and Their Applications. Springer Berlin Heidelberg, Berlin, 2008.
[16] Gross, B. and Zagier, D., On singular moduli, J. reine angew. Math 355 (1985), no.2, 191–220.
[17] Gross, B. and Zagier, D., Heegner points and derivatives of L-series, Invent. math 84 (1986), 225–320.
[18] A. Sutherland and J. Cremona, Computing the endomorphism ring of an elliptic curve over a number field, Contemporary Mathematics, 2023.
[19] D.A. Cox, Primes of the form $p = x^2 + ny^2$, 2nd edition, John Wiley and Sons, 2013.
[20] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves, GTM **151**, Springer, 1994.
[21] R. Schertz, Complex Multiplication, New Mathematical Monographs **15**, Cambridge Univ. Press, 2010.
[22] S. Lang, Elliptic functions. Springer New York, 1987.
[23] Dongxi Ye, Revisiting the Gross-Zagier discriminant formula, Math. Nachrichten, **293**, 2020, 1801–1826