Hilbert Class Polynomials

Badri Vishal Pandey
Supervisor : Prof Ken Ono

November 2019

1 Abstract

In my project I explored through first five sections of the paper **Traces of Singular Moduli** by **Don Zagier**. And as an application, we obtained a procedure to find **Hilbert class polynomials** without explicitly finding the roots.

2 Introduction

The values assumed by the modular invariant $j(\tau)$ at quadratic irrationality are called *Singular Moduli.* It turns out that these values are algebraic numbers. Then natural question that arises is: what is its minimal polynomial?. Instead of looking for these values, we can obtain results on their traces and a number of generalizations which can help us find these polynomials.

3 Preliminary

3.1 Positive Definite Binary Quadratic Forms

A binary quadratic form $q(x, y) = ax^2 + bxy + cy^2$, denoted by $[a, b, c]$ is called **positive definite** if it's **discriminant** $d = b^2 - 4ac$ is negative and $a > 0$. A discriminant is called **fundamental** if all the binary quadratic forms corresponding to it are primitive *i.e.* if $gcd(a, b, c) = 1$ for all such $[a, b, c]$.

Lemma. Let d be a given integer. d is a discriminant if and only if $d \equiv 0, 1(mod 4)$

3.2 Action of $\mathrm{PSL}_2\mathbb{Z}$ on Binary quadratic forms

Let $q(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic form. $\mathrm{PSL}_2\mathbb{Z}$ acts naturally on $q(x, y)$ by sending $q(x, y) \longrightarrow q(M(x, y)^t)$ for all matrices $M \in \mathrm{PSL}_2\mathbb{Z}$. If we look q as matrix then q correspond to matrix $Q = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$ in the sense that

$$q(x, y) = (x, y)Q(x, y)^t$$

with discriminant $d = -4\det(\mathrm{Q})$ Then the action by M corresponds to

$$(x, y)Q(x, y)^t \longrightarrow (x, y)M^tQM(x, y)^t$$

and $\det(M^tQM) = \det(Q)$ so this action preserves discriminant. So we get that this action produces infinitely many binary quadratic forms with discriminant d. Lets denote set of all binary quadratic forms with discriminant d by Q_d. As the action forms an equivalence relation, it divides Q_d in different equivalence classes. Gauss proved that the number of equivalence classes is finite.

Definition Let $q \equiv [a, b, c]$ be a binary quadratic form whose discriminant d is not a perfect square. We call q **reduced** if

$$-|a| \le b \le |a| < |c| \text{ or } 0 \le b \le |a| = |c|$$

It turns out that if your form is positive definite, each binary quadratic form corresponds to a unique *reduced form.* That is to say that each equivalence class has a unique reduced form in it.
Definition The number of equivalence classes of binary quadratic forms of discriminant d is called the **class number** of d, denoted by $h(d)$.

4 Hilbert Class Polynomials

Let $d > 0$ be a number such that $d \equiv 0, 3(mod4)$ then $-d$ is a discriminant. Let's also assume that $-d$ is fundamental discriminant so that all corresponding binary quadratic forms are primitive. And for simplicity, let Q_d be the set of all positive definite binary quadratic form (PDBQF) of discriminant $-d$. It turns out that in this case, each reduced form have a unique root in *fundamental domain* of $\mathrm{PSL}_2(\mathbb{Z})$ when you put $y = 1$(or more like a form is reduced if and only if it has a root in fundamental domain). So corresponding to $-d$, there are only finitely many points in fundamental domain. Then we define **Hilbert Class polynomial** of discriminant $-d$ as

$$H_d(X) = \prod_{Q \in Q_d/\Gamma} (X - j(\alpha_Q))$$

where α_Q is the unique root corresponding to equivalence class of Q in fundamental domain and $j(\tau)$ is modular invariant $j(\tau)$. It turns out that these polynomials are in $\mathbb{Z}[X]$ and are irreducible. More is known, that the splitting field K_d of this polynomial is maximal unramified galois extention over $\mathbb{Q}[\sqrt{-d}]$ and this field extension is called **Hilbert Class Field**. And more interesting fact is that corresponding Galois group is isomorphic to **Ideal Class group** of $\mathbb{Q}[\sqrt{-d}]$ *i.e* $\mathrm{Gal(K_d/\mathbb{Q}[\sqrt{-d}]) \cong CL(\mathbb{Q}[\sqrt{-d}])}$.
A more subtle question is how to calculate these polynomials? One way is(which was used as recently as mid '90s) : find all reduced quadratic forms of discriminant $-d$, find roots in upper half plane of each of them and then calculate $j-value$ at that point which seems quite tedious and not satisfactory because even these $j-values$ are not guaranteed to be integers(and people used to do approximations). Specially because there are $h(d)$ such calculations we have to do. And it's known that there are just 9 $d's$ $(3, 4, 7, 8, 11, 19, 43, 67, 163)$ such that $h(d) = 1$.
There is a more elegant way of calculating these polynomials just with the information of d and class number $h(d)$, which uses weakly holomorphic modular forms of weight 3/2 and/or 1/2.

5 Special weakly holomorphic modular forms of weight 1/2 and 3/2 and their relations

First we would like a formula for the trace of the roots of $H_d(X)$. For convenience we need to make two small changes. First, replace $j - invariant$ by the normalized Hauptmodul for $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$

$$J(\tau) = j(\tau) - 744 = q^{-1} + 196884q + 21493760q^2 + \cdots \quad \left(\tau \in \mathfrak{H}, q = e^{2\pi i\tau}\right)$$

Secondly, we weight the number $J(\alpha_Q)$ by the factor $1/\omega_Q$, where $\omega_Q = |\Gamma_Q|$(=2 or 3 if Q is $\Gamma - equivalent$ to $[1, 0, 1]$ or $[1, 1, 1]$ respectively, and 1 otherwise). Now We define the Hurwitz-Kronecker class numbers $H(d)$ and the modular trace function $\mathbf{t}(d)$ by

$$H(d) := \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{1}{w_Q}, \quad \mathrm{t}(d) := \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{1}{w_Q} J\left(\alpha_Q\right) \quad (d > 0, \quad d \equiv 0 \text{ or } 3 \pmod 4)$$

for example: we have
(1)$h(3) = 1$,$Q = [1, 1, 1]$, $\alpha = exp(2\pi i/3)$, so $j(\alpha) = 0$ and $H(3) = 1/3$ and $\mathrm{t}(3) = \dfrac{0 - 744}{3} = -248$
(2) $h(3) = 1$,$Q = [1, 0, 1]$, $\alpha = i$, so $j(\alpha) = 1728$ and $H(3) = 1/2$ and $\mathrm{t}(4) = \dfrac{1728 - 744}{3} = 492$
For some small values, we have

d	3	4	7	8	11	12	15	16	19
$H(d)$	1/3	1/2	1	1	1	4/3	2	3/2	2
$\mathbf{t}(d)$	−248	492	−4119	7256	−33512	53008	−192513	287244	−885480

d	20	23	24	27	28	31	32
$H(d)$	2	3	2	4/3	2	3	
$\mathbf{t}(d)$	1262512	−3493982	4833456	−12288992	16576512	−39493539	52255768

Now we look at a weight 3/2 weakly holomorphic modular form

$$\begin{aligned} g(\tau) :=& \theta_1(\tau)\frac{E_4(4\tau)}{\eta(4\tau)^6} \\ =& \frac{1}{q} - 2 + 248q^3 - 492q^4 + 4119q^7 - 7256q^8 + 33512q^{11} - 53008q^{12} + 192513q^{15} \\ & - 287244q^{16} + 885480q^{19} - 1262512q^{20} + 3493982q^{23} - 4833456q^{24} \\ & + 12288992q^{27} - 16576512q^{28} + 39493539q^{31} - 52255768q^{32} + \cdots \end{aligned}$$

where $\theta_1(\tau) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2}$ and E_4 and η are as usual.
We notice that first few coefficients of this $q-expansion$ are same as the traces of corresponding discriminants up-to sign. It turns out that this is not a coincidence. We have
Theorem Write the Fourier expansion of $g(\tau)$ as $g(\tau) = \sum_{d\geq -1} B(d)q^d$. Then

$$\mathbf{t}(d) = -B(d) \quad (\forall d > 0)$$

The idea of the proof is to look at: (1) $(g\theta)|U_4$ which is a holomorphic modular form of weight 2 hence should be identically 0. and (2) $[g,\theta]|U_4$, where $[g,\theta] = g'(\tau)\theta(\tau) - 3g(\tau)\theta'(\tau)$ which is a holomorphic modular form of weight 4 on $PSL_2(\mathbb{Z})$ and hence is a multiple of $E_4(\tau)$. From these two observations, we get

$$\sum_{r\in\mathbb{Z}} B\left(4n - r^2\right) = 0, \quad \sum_{r>0} r^2 B\left(4n - r^2\right) = 240\sigma_3(n) \quad (\forall n \geq 0)$$

where $\sigma_3(0) = 1/240$ and $\sigma_3(n)$ is as usual. From where we get recursions,

$$B(4n-1) = 240\sigma_3(n) - \sum_{2\leq r\leq\sqrt{4n+1}} r^2 B\left(4n - r^2\right), \quad B(4n) = -2\sum_{1\leq r\leq\sqrt{4n+1}} B\left(4n - r^2\right)$$

and we can get all the values by just $B(-1) = 240\sigma_3(0) = 1$
It turns out that the same identities are true for $\mathrm{t}(d)$. First identity uses the fact that

$$\Phi_n(X,X) = const. \times \prod_{|r|<2\sqrt{n}} \mathcal{H}_{4n-r^2}(X)$$

where

$$\Phi_n(X, j(\tau)) = \prod_{M\in\Gamma\backslash\mathcal{M}_n} (X - j(M\circ\tau)) \quad (\tau \in \mathfrak{H})$$

where $\mathcal{M}_n$ denotes the set of 2×2 matrices with determinant n in $PGL_2(\mathbb{Z})$.
And we equate $q-expansion$ of

$$\Phi_n(j(\tau), j(\tau)) = const. \times \prod_{|r|<2\sqrt{n}} \mathcal{H}_{4n-r^2}(j(\tau))$$

Second identity uses something which can be said to be analogous to taking log derivative of the above relation.
Now we got a nice formula for *traces*. But to get the whole polynomial, we need some more information.
The space of weakly holomorphic modular forms on half integer weights $(k + 1/2)$ is infinite dimensional for every k. In perticular, for every $d > 0$ with $d \equiv 0, 3(\mod 4)$ there is a unique modular form $f_d \in M^!_{1/2}$ having a q-expansion of the form

$$f_d(\tau) = q^{-d} + \sum_{D>0} A(D,d)q^D$$

and the functions $f_0, f_3, f_4, f_7, \ldots$ form a basis of $M^!_{1/2}$. These $f_i's$ are unique which is clear because $dim(M_{1/2} = 0$.
There is a procedure to calculate them. Namely, $f_0(\tau) = \theta(\tau)$ and a non-trivial linear combination of f_3 and f_0 can be obtained as $[\theta(\tau), E_{10}(4\tau)]/\Delta(4\tau)$, where $[\theta(\tau), E_{10}(4\tau)] = \theta(\tau)E'_{10}(4\tau) - 5\theta'(\tau)E_{10}(4\tau)$. Comparing $q-coefficients$, we get f_3. And now for each $d \geq 4$ we obtain $f_d(\tau)$ by multiplying $f_{d-4}(\tau)$ by $j(4\tau)$ to get a plus-form of weight 1/2 with leading coefficient q^{-d} and then diagonalizing it using previous $f_{d'}s$.We have Fourier expansions of the first few f_d begin as follows:

$$\begin{aligned}
f_0 =& 1 + 2q + 2q^4 + 2q^9 + 2q^{16} + \mathrm{O}\left(q^{25}\right)\\
f_3 =& q^{-3} - 248q + 26752q^4 - 85995q^5 + 1707264q^8 - 4096248q^9 + \mathrm{O}\left(q^{12}\right)\\
f_4 =& q^{-4} + 492q + 143376q^4 + 565760q^5 + 18473000q^8 + 51180012q^9 + \mathrm{O}\left(q^{12}\right)\\
f_7 =& q^{-7} - 4119q + 8288256q^4 - 52756480q^5 + 5734772736q^8 + \mathrm{O}\left(q^9\right)
\end{aligned}$$

In a similar way we can define a second sequence of unique modular forms of 3/2 integer weight for every integer $D > 0$ with $D \equiv 0, 1(\mod 4)$ having $q-expansion$ like

$$g_D(\tau) = q^{-D} + \sum_{d\geq 0} B(D,d)q^d$$

$g_1(\tau)$ is just $g(\tau)$ we defined earlier and we can construct g_4 just like in the case of $f_i's$ by obtaining $\left[g_1(\tau), E_{10}(\tau)\right]/\Delta(4\tau)$ as a linear combination of $g_1(\tau), g_4(\tau)$, and $g_1(\tau)j(4\tau)$. And rest by by multiplying $g_{D-4}(\tau)$ by $j(4\tau)$ and diagonalizing.

$$\begin{aligned}
g_1 =& q^{-1} - 2 + 248q^3 - 492q^4 + 4119q^7 - 7256q^8 + 33512q^{11} - 53008q^{12} + \mathrm{O}\left(q^{15}\right) \\
g_4 =& q^{-4} - 2 - 26752q^3 - 143376q^4 - 8288256q^7 - 26124256q^8 + \mathrm{O}\left(q^{11}\right) \\
g_5 =& q^{-5} + 0 + 85995q^3 - 565760q^4 + 52756480q^7 - 190356480q^8 + \mathrm{O}\left(q^{11}\right) \\
g_8 =& q^{-8} + 0 - 1707264q^3 - 18473000q^4 - 5734772736q^7 - 29071392966q^8 + \mathrm{O}\left(q^{11}\right)
\end{aligned}$$

Theorem (Borcherds) . Let $d > 0, d \equiv 0$ or 3 (mod 4). Then

$$\mathcal{H}_d(j(\tau)) = q^{-H(d)} \prod_{n=1}^{\infty} \left(1 - q^n\right)^{A\left(n^2, d\right)}$$

Comparing Borcherds Theorem with the formula for weighted $H_d(j(\tau))$, we get
Corollary. $\mathbf{t}(d) = A(1, d)$ for all $d > 0$.
And from previous results, we have $\mathbf{t}(d) = -B(1, d)$
So we get a relation

$$A(1, d) = -B(1, d)$$

More generaly

$$A(D, d) = -B(D, d)$$

Let's define functions J_m for every integer $m \geq 0$ as the unique holomorphic function on $\mathfrak{H}/\Gamma$ with a Fourier expansion beginning $q^{-m} + \mathrm{O}(q)$. For $m = 0$ this is the constant function 1 and for $m = 1$ it is the function $J(\tau) = j(\tau) - 744$. And

$$\begin{aligned}
J_2(\tau) &= q^{-2} + 42987520q + 40491909396q^2 + 8504046600192q^3 + \cdots \\
J_3(\tau) &= q^{-3} + 2592899910q + 12756069900288q^2 + 9529320689550144q^3 + \cdots \\
J_4(\tau) &= q^{-4} + 80983425024q + 1605963589611520q^2 + 3497254878743101440q^3 + \cdots
\end{aligned}$$

As being modular forms of weight 0, we have J_m can be written as a polynomial in $j(\tau)$. We get first few J_m

$$\begin{aligned}
J_2(\tau) =& j(\tau)^2 - 1488j(\tau) + 159768 \\
J_3(\tau) =& j(\tau)^3 - 2232j(\tau)^2 + 1069956j(\tau) - 36866976 \\
J_4(\tau) =& j(\tau)^4 - 2976j(\tau)^3 + 2533680j(\tau)^2 - 561444608j(\tau) + 8507424792
\end{aligned}$$

We define analogous to traces of higher powers,

$$\mathbf{t}_m(d) := \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{1}{w_Q} J_m\left(\alpha_Q\right)$$

Now to get a formula for $t_m(d)$ we need to involve Hecke operators. For any integer $m \geq 1$ let $A_m(D, d)$ and $B_m(D, d)$ denote the coefficient of q^D in $f_d|_{\frac{1}{2}} T(m)$ and the coefficient of q^d in $g_D|_{\frac{3}{2}} T(m)$, respectively. Then we have
Theorem. With the above notations, we have
(i) $\mathcal{H}_d(j(\tau)) = q^{-H(d)} \exp\left(-\sum_{m=1}^{\infty} \mathrm{t}_m(d) \frac{q^m}{m}\right)$ for all d
(ii) $\mathrm{t}_m(d) = -B_m(1, d)$ for all m and d
(iii) $A_m(D, d) = -B_m(D, d)$ for all m, D and d
Now we have enough tools to tackle our main goal.

6 Calculating Hilbert Class Polynomials

Let

$$P_m(d) = \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{1}{w_Q} j\left(\alpha_Q\right)^m$$

Then we have $p_0(d) = H(d)$,$P_1(d) = t(d)$ and inductively from the fact that $J_m(\tau)$ are polynomials in $j(\tau)$, we can get

$$P_m(d) = t_m(d) + \text{linear combination of } P_0(d), P_1(d), \cdots P_m(d)$$

Now if our Hilbert class polynomial looks like

$$H_d(X) = \sum_{n=0}^{h(d)} (-1)^{h(d)-n} e_n(d) X^n$$

Then by **Newton–Girard formulae**, we have $e_0(d) = 1$, $e_1(d) = P_1(d) = t(d)$ and inductively,

$$e_k(d) = \frac{1}{k} \sum_{i=1}^{k-1} (-1)^{i-1} e_{k-i}(d) P_i(d)$$

7 Some Examples

(1) $d = 3, h(3) = 1, t_1(3) = -248$

$$H_3(X) = X + 248$$

(2) $d = 15, h(15) = 2,$
$t_1(15) = B_1(1, 15) = -192513$
As $J_1(\tau) = j(\tau) - 744,$
$P_1(15) = t_1(15) + h(15) * 744 = -191025$
As $J_2(\tau) = j(\tau)^2 - 1488 * j(\tau) + 159768$
$P_2(15) = t_2(15) + 1488 * P_1(15) - 159768 * h(15) = -B_2(1, 15) + 1488 * P_1(15) - 159768 * h(15) = 3701760111$
$e_1(15) = P_1(15) = -191025$
$e_2(15) = \frac{1}{2}(e_1(15) * P_1(15) - e_0(15) * P_2(15)) = -121287375$

$$H_{15}(X) = X^2 + 191025X - 121287375$$

(3) $d = 23, h(23) = 3,$
$t_1(23) = B_1(1, 23) = -3493982$
$P_1(23) = t_1(23) + h(23) * 744 = -3491750$
$P_2(23) = t_2(23) + 1488 * P_1(23) - 159768 * h(23) = -B_2(1, 23) + 1488 * P_1(23) - 159768 * h(23) = 12202620656250$
$P_3(23) = t_3(23) + 2232 * P_2(23) - 1069956 * P_1(23) + 36866973 * h(23) = -B_3(1, 23) + 2232 * P_2(23) - 1069956 * P_1(23) + 36866973 * h(23) = -4262652603296796875$
$e_1(23) = P_1(23) = -3491750$
$e_2(23) = \frac{1}{2}(e_1(23) * P_1(23) - e_0(23) * P_2(23)) = -5151296875$
$e_3(23) = \frac{1}{3}(e_2(23)P_1(23) - e_1(23)P_2(23) + e_0(23)P_3(23)) = -12771880859375$

$$H_{23}(X) = x^3 + 3491750x^2 - 5151296875x + 12771880859375$$

(4)$H_{71}(X) = x^7 + 313645809715x^6 - 3091990138604570x^5 + 98394038810047812049302x^4 - 823534263439730779968091389x^3 + 5138800366453976780323726329446x^2 - 425319473946139603274605151187659x + 737707086760731113357714241006081263$