Quadratic Imaginary Fields of Class Number 1

Wednesday, 30 September 2020 23:38

Class Number of quadratic orders

Let $K = \mathbb{Q}[\sqrt{n}]$, $n>1$ is squarefree. Notation: $[\alpha, \beta] := \mathbb{Z}\alpha \oplus \mathbb{Z}\beta$

Maximal order $\mathcal{O}_K = [1, w_K]$, $w_K = \dfrac{d_K + \sqrt{d_K}}{2}$

where $d_K = \begin{cases} n & n \equiv 1 \pmod 4 \\ 4n & \text{otherwise} \end{cases}$

For an order $\mathcal{O}$, define conductor $f := [\mathcal{O}_K : \mathcal{O}] < \infty$

then, $\mathcal{O} = [1, f w_K]$ and has discriminant $D = f^2 d_K$

The discriminant D determines $\mathcal{O}$ uniquely & any non-square $D \equiv 0, 1 \pmod 4$ is the discriminant of an order

$I(\mathcal{O})$ = group of invertible fractional ideals of $\mathcal{O}$

$P(\mathcal{O})$ = group of principal fractional ideals of $\mathcal{O}$

Then, $P(\mathcal{O}) \subseteq I(\mathcal{O})$ and the class group $C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$

$h(\mathcal{O}) := |C(\mathcal{O})|$ is class number, sometimes denoted as $h(D)$

We want to find all $n \in \mathbb{Z}_{\geq 0}$ such that $h(-n) = 1$

The following formula relates $h(\mathcal{O})$ to $h(\mathcal{O}_K)$

$$(*) \quad h(\mathcal{O}) = \frac{h(\mathcal{O}_K)\, f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{\substack{p \mid f \\ p \text{ prime}}} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right)$$

where: odd p $\quad \left(\dfrac{d_K}{p}\right) = \begin{cases} 0 & p \mid d_K \\ 1 & d_K \text{ is quadratic residue mod } p \\ -1 & \text{otherwise} \end{cases}$

$p=2$ $\quad \left(\dfrac{d_K}{2}\right) = \begin{cases} 0 & d_K \text{ even} \\ 1 & d_K \equiv \pm 1 \pmod 8 \\ -1 & d_K \equiv \pm 3 \pmod 8 \end{cases}$

Using the theory of quadratic forms one shows:

Using the theory of quadratic forms one shows:

Thm A: For $n \in \mathbb{Z}_{>0}$ $\quad h(-4n) = 1 \iff n = 1, 2, 3, 4, 7$

Thm B: For $n \in \mathbb{Z}_{>0}$ such that n has atleast two odd prime factors we have $h(-n)$ is even

Thm A gives a complete list of all imaginary quadratic orders with even discriminant that have class number 1

Among the imaginary quadratic orders with odd discriminant, by Thm B, only those with (negative) prime discriminant can have class number 1. We seperate them into the following two cases
(i) $p \equiv 7 \pmod 8$ $\qquad$ (ii) $p \equiv 3 \pmod 8$

In both these cases, the order with discriminant $-p$ is maximal
$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ where $K = \mathbb{Q}[\sqrt{-p}]$

This contains the order $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ which has discriminant $-4p$
Using formula ⊛ we obtain

$$h(-4p) = 2\,h(-p)\left(1 - \left(\frac{-p}{2}\right)\frac{1}{2}\right)$$

as $\mathcal{O}_K^\times = \mathcal{O}^\times = \{\pm 1\}$ (elements with norm 1)
$-4p = (2)^2(-p) \implies f = 2$

For case (i): $\left(\frac{-p}{2}\right) = 1 \implies h(-4p) = h(-p) \overset{\text{(assume)}}{=} 1$

Then, by Thm A we obtain $p = 7$.

For case (ii): $\left(\frac{-p}{2}\right) = -1 \implies h(-4p) = 3h(-p) = 3$

To proceed further we need to use the theory of complex multiplication

Main Theorem:
Let $\mathcal{O}$ = imaginary quadratic order, $\mathfrak{a}, \mathfrak{b}$ = invertible fractional $\mathcal{O}$-ideals
① $j(\mathfrak{a})$ is an algebraic integer and $L = K(j(\mathfrak{a}))$

Let $\mathcal{O}$ = imaginary quadratic order, a, b = invertible fractional $\mathcal{O}$-ideals

① $j(a)$ is an algebraic integer and $L = K(j(a))$ is the ring class field of $\mathcal{O}$

② The isomorphism between $C(\mathcal{O})$ and $Gal(L/K)$ is given by

$$a \mapsto \sigma_a$$

where $\sigma_a \in Gal(L/K)$ is determined by the following

$$\sigma_a(j(b)) = j(\bar{a}b) \quad [\bar{a} \text{ is conjugate of } a]$$

In case (ii), if we choose the order $\mathcal{O} = \mathbb{Z}(\sqrt{-p})$ then the Main Theorem implies that $L = K(j(\sqrt{-p}))$ is the ring class field of $\mathcal{O}$

We want to have another description of L involving different modular functions which we will now define

The modular function γ_2 :

The j-function is non-vanishing holomorphic function on the simply connected domain $\mathbb{H}$ and hence admits a logarithm. Define $\gamma_2(z)$ to be the cube root of $j(z)$ satisfying the property that $\gamma_2(iy) \in \mathbb{R}$ $\forall\, y \in \mathbb{R}_{>0}$ (note that the j function satisfies this property because it has a q-expansion with integer coefficients)

Thm. $\gamma_2(z)$ is a modular function for the congruence subgroup

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{matrix} a \equiv d \equiv 0 \pmod 3 \text{ or} \\ b \equiv c \pmod 3 \end{matrix} \right\}$$

Thm 1 Let $\mathcal{O} = [1, \tau_0]$ be the imaginary quadratic order of discriminant D. If $3 \nmid D$ then $\gamma_2(\tau_0)$ is an algebraic integer and $K(\gamma_2(\tau_0))$ is the ring class field of $\mathcal{O}$

The following consequence of this Thm is important for us

In case (ii), we can choose the order $\mathcal{O}_K = [1, \frac{3+\sqrt{-p}}{2}]$

which we assumed to have class number 1 and hence which we assumed to have class number 1 and hence

$(\clubsuit)$ For $\tau_0 = \frac{3+\sqrt{-p}}{2}$ we have $\gamma_2(\tau_0) \in \mathbb{Z}$

Weber's functions:

We define the following functions :

$$f(z) := q^{-1/48} \prod_{n=1}^{\infty} \left(1 + q^{(n-1)/2}\right)$$

$$f_1(z) := q^{-1/48} \prod_{n=1}^{\infty} \left(1 - q^{(n-1)/2}\right)$$

$$f_2(z) := \sqrt{2}\, q^{1/24} \prod_{n=1}^{\infty} \left(1 + q^{n}\right)$$

These functions satisfy the following transformation properties

Thm:

$$f(z+1) = \zeta_{48}^{-1} f_1(z) \qquad f\left(-\tfrac{1}{z}\right) = f(z)$$

$$f_1(z+1) = \zeta_{48}^{-1} f(z) \qquad f_1\left(-\tfrac{1}{z}\right) = f_2(z)$$

$$f_2(z+1) = \zeta_{24} f_2(z) \qquad f_2\left(-\tfrac{1}{z}\right) = f_1(z)$$

These functions can also be used to compute the function $\gamma_2(z)$

Thm: (Δ)

$$\gamma_2(z) = \frac{f(z)^{24} - 16}{f(z)^8} = \frac{f_1(z)^{24} + 16}{f_1(z)^8} = \frac{f_2(z)^{24} + 16}{f_2(z)^8}$$

We use the transformation properties of $f(z)$ as mentioned above and the product formula given in the definition (to check meromorphicity at cusps) to obtain

Thm $f(8z)^6$ is a modular function for $\Gamma_0(64)$

Next, we want to invoke the following well known fact

Thm If $g(z)$ is a modular function for $\Gamma_0(N)$ then $g(z) \in \mathbb{C}(j(z), j(Nz))$ [rational function]

Moreover, if $g(z)$ has a rational q expansion then

$g(z) \in \mathbb{C}(j(z), j(Nz))$ [rational function]

Moreover, if $g(z)$ has a rational q expansion then

$$g(z) \in \mathbb{Q}(j(z), j(Nz))$$

Combining the previous two results we obtain that

$$⬠ \quad f(8z)^6 = R(j(64z), j(z)), \text{ for } R \in \mathbb{Q}(x,y)$$

Now we are ready to prove the following result

Thm 2 Let $m \equiv 3 \pmod 4$ and $\mathcal{O} = [1, \sqrt{-m}]$. Then
$f(\sqrt{-m})^2$ is an algebraic integer
$K(f(\sqrt{-m})^2)$ is the ring class field of $\mathcal{O}$

Proof. Let L denote the ring class field of $\mathcal{O}$.
First, we want to show that $f(\sqrt{-m})^6 \in L$
In ⬠ we substitute $z = \sqrt{-m}/8$ to obtain

$$f(\sqrt{-m})^6 = R(j(8\sqrt{-m}), j(\sqrt{-m}/8))$$

Note that $\underset{\text{invertible ideal}}{[1, \sqrt{-m}/8]} \subseteq \underset{\text{order}}{[1, 8\sqrt{-m}] = \mathcal{O}'}$

Hence, by the Main Theorem, $j(\sqrt{-m}/8), j(8\sqrt{-m}) \in L'$
where L' = ring class field of $\mathcal{O}'$

This gives us that $f(\sqrt{-m})^6 \in L' \supseteq L$
To show that $f(\sqrt{-m})^6 \in L$, we need to show that it is invariant under $Gal(L'/L)$
We can compute $Gal(L'/L)$ explicitly as the kernel of

$$C(\mathcal{O}') \longrightarrow C(\mathcal{O})$$

It turns out to be isomorphic to the group $\mathbb{Z}/4 \times \mathbb{Z}/2$ with generators $a = [8, 2+\sqrt{-m}]$, $b = [8, \sqrt{-m}]$ resp.
We need to show $R(j(8\sqrt{-m}), j(\sqrt{-m}/8))$ is fixed by σ_a, σ_b (using the notation of Main Theorem)

$$\sigma_a(R(j([1, 8\sqrt{-m}]), j([8, \sqrt{-m}])))$$

$$\overset{\text{def + Q-lin}}{=} R(j(\bar{a}[1, 8\sqrt{-m}]), j(\bar{a}[8, \sqrt{-m}]))$$

$$\underset{\text{calculation}}{\overset{\text{explicit}}{=}} R(j([4, 3+2\sqrt{-m}]), j([8, 6+\sqrt{-m}])) \quad \text{I}$$

$\overset{\text{calculation}}{=} \quad R(j([4, 5+2\sqrt{-m}]), j([8, 8+\sqrt{-m}])) \qquad \mathrm{I}$

$$\begin{aligned}
&\gamma_b(R(j[1, 8\sqrt{-m}]), j([8, \sqrt{-m}])))\\
\overset{\text{def} + \mathbb{Q}\text{-lin}}{=}\ & R(j(\bar{b}[1, 8\sqrt{-m}]), j(\bar{b}[8, \sqrt{-m}]))\\
\overset{\text{explicit calculation}}{=}\ & R(j([1, 8\sqrt{-m}]), j([8, \sqrt{-m}])) \qquad \mathrm{II}
\end{aligned}$$

We have used $m \equiv 3 \pmod 4$ in the above calculations

Let $\gamma_1 = \begin{pmatrix} 2 & 11 \\ 1 & 6 \end{pmatrix}$ and $\gamma_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$

We can explicitly check that

$$\mathrm{I} = f(\gamma_1 \cdot \sqrt{-m})^6 \qquad \mathrm{II} = f(\gamma_2 \cdot \sqrt{-m})^6$$

Now, using the transformation properties of $f(z)$ as given before we get $f(\gamma_1 \cdot \sqrt{-m})^6 = f(\gamma_2 \cdot \sqrt{-m})^6 = f(\sqrt{-m})^6$

Hence we obtain $f(\sqrt{-m})^6 \in L$

Using Δ we have

$$f(\sqrt{-m})^{24} - f(\sqrt{-m})^8 \gamma_2(\sqrt{-m}) - 16 = 0$$

3∤D?

By Thm 1, $\gamma_2(\sqrt{-m}) \in L$. Combining this with $f(\sqrt{-m})^{24} \in L$

we obtain $f(\sqrt{-m})^8 \in L \Rightarrow \dfrac{f(\sqrt{-m})^8}{f(\sqrt{-m})^6} = f(\sqrt{-m})^2 \in L$

Using the above equation again, we obtain

$$j(\sqrt{-m}) = \gamma_2(\sqrt{-m})^3 = \left(\frac{f(\sqrt{-m})^{24} - 16}{f(\sqrt{-m})^8}\right)^3 \in K(f(\sqrt{-m})^2)$$

Hence, $\underset{(\text{Main Thm})}{L = K(j(\sqrt{-m}))} \underset{(\text{by above})}{\subseteq} K(f(\sqrt{-m})^2) \underset{(f(\sqrt{-m})^2 \in L)}{\subseteq} L$

This completes the proof.

////

Now we have Thm 1 and Thm 2 which give us a different description of the ring class field L and we can proceed to Heegner's proof for case (ii)

Heegner's Proof (Use notation of case (ii))

Let L denote the ring class field of order $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$

We have shown $h(-4p) = 3$ and hence $[L:K] = 3$

By Thm 2, $L = K(f(\sqrt{-p})^2)$

Let $\tau_0 = \dfrac{3+\sqrt{-p}}{2}$ and $\alpha = \zeta_8^{-1} f_2(\tau_0)^2 \underset{\text{Weber functions}}{\overset{\text{properties of}}{=\!=\!=}} \dfrac{2}{f(\sqrt{-p})^2}$

Hence, $\alpha \in L \setminus K$ and α is degree 3 over K

But, $f(\sqrt{-p}) \in \mathbb{R}$ (rational q-expansion)

Hence $\alpha \in \mathbb{R}$ and is degree 3 over $\mathbb{Q}$.

From Δ it follows that $\alpha^4 = -f_2(\tau_0)^8$ is a root of

$$x^3 - \gamma_2(\tau_0)x - 16 = 0$$

By (✿) we have that $\gamma_2(\tau_0) \in \mathbb{Z}$ and hence both α, α^4 are algebraic integers. Let α be a root of

$$x^3 + ax^2 + bx + c = 0 \qquad a, b, c \in \mathbb{Z}$$

Seperating the even and odd degree terms and squaring we obtain a cubic polynomial with integer coefficients having α^2 as a root.

Repeating this once again, we obtain the same for α^4.

Comparing this with $x^3 - \gamma_2(\tau_0)x - 16$ we get a system of Diophatine equations in a, b, c & $\gamma_2(\tau_0)$ which can be shown by elementary methods to have only finitely many solutions.

Hence we obtain only finitely many values for $j(\tau_0)$

As the value of $j(\tau_0)$ determines the order uniquely, we obtain that there are only finitely many quadratic orders with class number 1.

It is possible to compute $j(\tau_0)$ for

$$p = 11, 19, 43, 67, 163$$

It is possible to compute $j(\tau_0)$ for

$$p = 11, 19, 43, 67, 163$$

and we obtain all possible values of $j(\tau_0)$ (which are solutions to the system of Diophantine equations) in this list. Hence, these are all quadratic imaginary orders with class number 1 and discriminant $-p$ where $p \equiv 3 \pmod 8$. This finishes the proof.