Classification of Imaginary Quadratic Fields of Class Number 1

§1. The Class Number

1.1. Quadratic Forms (Q_D^+/Γ , reduced forms, etc.)

1.1.2. Landau's Theorem

1.1.3. Class group $Cl(D)$ and the 2-torsion part.

1.2. Orders

1.2.1. Definitions and basic properties (conductor, discriminant, etc.)

1.2.2. The class group $Cl(\mathcal{O})$ and the isomorphism $Cl(\mathcal{O}) \cong Cl(D)$

1.2.3. The class number formula.

§2. Automorphic Functions

2.1. Definitions of automorphic/modular forms (graded algebra $\mathcal{A}(\Gamma_0(N))$)

2.2. Examples: $G_K, \Delta, \eta, j, \gamma_2, \mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2$ (the Weber functions)

2.3. Relations between $\gamma_2, \mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2$

2.4. Computation of $j(\mathcal{O})$ for $h(\mathcal{O}) = 1$ using $\gamma_2, \mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2$

2.5. Complex Multiplication: generating ring class fields with special values of $\gamma_2, \mathfrak{f}, \ldots$

§3. Main Theorem

3.1. Statement, discussion about why it might be true (Siegel's formula, Gross-Zagier) + history about its proof.

3.2. Proof of ($\Leftarrow$) using computers and quadratic forms.

3.3. Reduction to the case $d_K = -p$, $p \equiv 3 \pmod 8$

3.4. Study the field theoretic properties of $\alpha = \zeta_8 \mathfrak{f}_2\left(\frac{3+\sqrt{-p}}{2}\right)^2$

3.5. Solve the diophantine equations deduced from 3.4

3.6. Produce a list of j-invariants and compare to 2.4

1.1. Quadratic Forms

- DEF: • An integral binary quadratic form is a polynomial $Q(x,y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x,y]$.
  - it is primitive if $\gcd(a,b,c) = 1$
  - the discriminant of Q is $D = b^2 - 4ac$ ~~(we will only consider~~
  - Q is positive definite if $D < 0$, $a > 0$
  - A form Q is reduced if it is primitive, positive definite and $|b| \le a \le c$, $|b| = a$ or $a = c \Rightarrow b \geq 0$

  Note: if Q is reduced $\Rightarrow \sqrt{\frac{-D}{3}} \geq a \geq |b|$ so there are finitely many reduced forms of a given discriminant.

  Note: ↑ gives an algorithm to explicitly write all reduced forms of discriminant D.

- There is an action $\overbrace{SL_2(\mathbb{Z})}^{\Gamma} \curvearrowright Q_D^+ = \{ Q \mid Q \text{ is prim., pos. def. and disc} = D \}$

$$(\gamma . Q)(x,y) = Q(px+qy, rx+sy) \quad , \quad \gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

PROP: {reduced forms of disc D} is a complete set of representatives for $\Gamma \curvearrowright Q_D^+$

DEF: $Cl(D) = \Gamma \backslash Q_D^+$ and it is a group with the composition law

$$(Q * Q')(x,y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'} y^2 \qquad \text{(B satisfies some system of congr.)}$$

$$[Q] \cdot [Q^*] = [Q * Q'] \quad , \quad [ax^2 + bxy + cy^2]^{-1} = [ax^2 - bxy + cy^2]$$

NOTE: the simple description of $[Q]^{-1}$ gives us a very simple description of $Cl(D)[2]$. in fact:

$\boxed{\text{PROP}}$: $D \equiv 1 \pmod 4 \Rightarrow |Cl(D)[2]| = 2^{r-1}$ (r = # of prime divisors of D)

- $\boxed{\text{THM (Landau)}}$ $h(-4n) = 1 \iff n \in \{1,2,3,4,7\}$

Pf: $\Leftarrow$| Computational (e.g. $n = 3$, $D = -12$, $\sqrt{\frac{-D}{3}} = 2 \geq a \geq |b|$

$$\begin{cases} a = 2 \Rightarrow b \in \{-1,0,1,2\} \\ a = 1 \Rightarrow b \in \{0,1\} \\ c = \frac{b^2 - D}{4a} \in \mathbb{Z} \end{cases}$$

$\Rightarrow$| If $n \neq 1,2,3,4,7$ you explicitly construct at least two reduced forms of discriminant $-4n$.

- $x^2 + ny^2$ is always one
- $n = ac$ (not prime power), $\gcd(a,c) = 1 \Rightarrow ax^2 + cy^2$ works
- $n = 2^r$ $r \geq 4$, $4x^2 + 4xy + (2^{r-1}+1)y^2$ works, etc...

1.2 - Orders

- Recall: K is an imaginary quadratic field, $K = \mathbb{Q}(\sqrt{D})$, $D<0$ $\square$-free

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & D \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{D}] & D \not\equiv 1 \pmod 4 \end{cases}, \quad d_K = \begin{cases} D & D\equiv 1 \pmod 4 \\ 4D & D \not\equiv 1 \pmod 4 \end{cases}, \quad \mathcal{O}_K^\times = \{\pm 1\} \ (D<-3)$$

- <u>DEF</u>: $\mathcal{O} \subseteq K$ is an order in K if it is a subring & contains an integral basis for $K/\mathbb{Q}$.

Remarks:

- $\mathcal{O} \subseteq \mathcal{O}_K$ by the integrality of $\mathcal{O}_K$
- $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 2

$\Rightarrow [\mathcal{O}_K : \mathcal{O}] = f < \infty$ is called the conductor of D.

$\hookrightarrow \mathcal{O} = \langle 1, f\omega_K \rangle \quad \omega_K = \frac{d_K + \sqrt{d_K}}{2}$ so the conductor uniquely determines $\mathcal{O}$.

- $D := \det\begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \end{pmatrix}^2 = f d_K$ is called the discriminant of $\mathcal{O} = \langle \alpha, \beta \rangle$

$D = -4V^2$, $V =$ volume $\langle \alpha, \beta \rangle$.

<u>DEF</u>: $I(\mathcal{O}) = \{\mathfrak{a} \subseteq K \mid \mathfrak{a}$ is an <u>invertible</u> fractional ideal$\}$, $P(\mathcal{O}) = \{\mathfrak{a} \in I(\mathcal{O}) \mid \mathfrak{a}$ is principal$\}$

fractional ideal: $\neq 0$, f.g. $\mathcal{O}$-submodule of K.

Note: $\mathcal{O} = \mathcal{O}_K$ then frac. ideal $\Rightarrow$ invertible frac. ideal. $\leftarrow$ ($\not\Leftarrow$, $\mathcal{O} = \langle 1, \sqrt{-3} \rangle$, $\mathfrak{a} = \langle 2, 1+\sqrt{-3} \rangle$).

<u>DEF</u>: $I(\mathcal{O})$ is a group with $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a}\mathfrak{b}$, $P(\mathcal{O})$ is a subgroup, $Cl(\mathcal{O}) := \frac{I(\mathcal{O})}{P(\mathcal{O})}$

$h(\mathcal{O}) = |Cl(\mathcal{O})|$

<u>Example</u>: $\mathcal{O} = \mathbb{Z}[\sqrt{-3}] \subset \mathbb{Q}(\sqrt{-3})$ has $d_K = -12$. We will see $h(\mathcal{O}) = 1$ but $\mathcal{O}$ is not a UFD (e.g. $2 \cdot 2 = 4 = (1+\sqrt{-3})(1-\sqrt{-3})$). This is a big difference between $\mathcal{O}$ and $\mathcal{O}_K$.

<u>THM</u>: $D<0$, $D \equiv 0,1 \pmod 4$. $\mathcal{O} \subseteq K$ disc $= D$ then $Cl(D) \cong Cl(\mathcal{O})$ via:

$$[ax^2 + bxy + cy^2] \longmapsto \left\langle a, \frac{-b+\sqrt{D}}{2} \right\rangle, \quad \langle \alpha, \beta \rangle \mapsto \frac{N_{K/\mathbb{Q}}(\alpha x - \beta y)}{N(\langle \alpha, \beta \rangle)} \quad (\operatorname{Im}(\beta/\alpha) > 0)$$

Remarks:

- it is necessary for K to be imaginary: e.g. $K = \mathbb{Q}(\sqrt{3})$ is a UFD so $h(\mathcal{O}_K) = 1$ but $h(12) > 1$ since $\pm(x^2 - 3y^2)$ are inequivalent forms. To remedy this we only consider the <u>narrow class group</u> $C^+(\mathcal{O}) := I(\mathcal{O}) / P^+(\mathcal{O})$ where $P^+(\mathcal{O}) = \{\alpha\mathcal{O} \mid N(\alpha) > 0\}$

1.2 - Orders

THM: (Class number formula) $$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \frac{|(\mathcal{O}_K/f\mathcal{O}_K)^\times|}{|(\mathcal{O}/f\mathcal{O})^\times|}$$

For K imaginary quadratic:

Legendre symbol for odd p

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \cdot f \prod_{p \mid f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right) \qquad \left(\frac{d_K}{2}\right) = \begin{cases} 0 & 2 \mid d_K \\ 1 & d_K \equiv 1 \ (8) \\ -1 & d_K \equiv 5 \ (8) \end{cases}$$

Pf (Sketch) There is an exact sequence ~~given by the~~ $1 \to \mathcal{O}^\times \to \mathcal{O}_K^\times \to \frac{(\mathcal{O}_K/f\mathcal{O}_K)^\times}{(\mathcal{O}/f\mathcal{O})^\times} \to C(\mathcal{O}) \to C(\mathcal{O}_K) \to 1$ given by the snake lemma applied to

$$\begin{tikzcd}
1 \arrow[r] & K^\times/\mathcal{O}^\times \arrow[r] \arrow[d] & \bigoplus_{\mathfrak{p} \subset \mathcal{O}} K^\times/\mathcal{O}_\mathfrak{p} \arrow[r] \arrow[d] & C(\mathcal{O}) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & K^\times/\mathcal{O}_K^\times \arrow[r] & \bigoplus_{\mathfrak{p} \subset \mathcal{O}_K} K^\times/(\mathcal{O}_K)_\mathfrak{p} \arrow[r] & C(\mathcal{O}_K) \arrow[r] & 1
\end{tikzcd}$$

and $\bigoplus_{\mathfrak{p} \subset \mathcal{O}} (\mathcal{O}_K)_\mathfrak{p}^\times / \mathcal{O}_\mathfrak{p}^\times \cong (\mathcal{O}_K/f\mathcal{O}_K)^\times / (\mathcal{O}/f\mathcal{O})^\times$ by CRT. $\square$

COR: Using $Cl(D) \leftrightarrow Cl(\mathcal{O})$ we have $\boxed{h(m^2 D) = h(D)\, m \prod_{p \mid m} \left(1 - \left(\frac{D}{p}\right)\frac{1}{p}\right)}$

Pf: Take $\mathcal{O}$ and $\mathcal{O}'$ of $[\mathcal{O}:\mathcal{O}'] = m$ and compare $h(\mathcal{O})$ and $h(\mathcal{O}')$ to $h(\mathcal{O}_K)$.
Note: $\mathcal{O}_K^\times = \pm 1$ when $D < -3$.

Example $\mathcal{O} = \mathbb{Z}[\sqrt{-5}] = \mathcal{O}_K$, $K = \mathbb{Q}(\sqrt{-5})$, $D = -20$ and ${}_p\mathcal{Q}^+_{-20} = \{[x^2+5y^2], [2x^2+2xy+3y^2]\}$

so $Cl(-20) = \{1, \langle 2, 1+\sqrt{-5}\rangle\}$.

§ 2. Modular(ish) Functions

DEF: $j : \mathbb{H} \to \mathbb{C}$ by $j(z) = j(\langle z, 1 \rangle) = 1728 \dfrac{g_2(z)^3}{\Delta(z)}$

Remarks: The Weierstrass $\wp$-function satisfied the diff. eqn. $(\wp_\Lambda')^2 = 4\wp_\Lambda^3 - g_2(\Lambda)\wp - g_3(\Lambda)$ where $g_k(\Lambda) = \sum_{\omega \in \Lambda \setminus 0} \frac{1}{\omega^{2k}}$ and $\Delta(\Lambda)$ is the discriminant of the polynomial $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$, i.e. $\Delta(z) = 16(e_1-e_2)^2(e_1-e_3)^2(e_2-e_3)^2$ where $e_1 = \wp_\Lambda(\frac{\omega_1}{2})$, $e_2 = \wp_\Lambda(\frac{\omega_2}{2})$, $e_3 = \wp_\Lambda(\frac{\omega_1+\omega_2}{2})$, $\Lambda = \langle \omega_1, \omega_2 \rangle \Rightarrow \Delta(\Lambda) \neq 0$.

Properties:

- $j(\mathcal{O}) \in \mathbb{R}$ (follows from $\mathcal{O} = \overline{\mathcal{O}}$, and $\overline{j(\Lambda)} = j(\overline{\Lambda})$) / $j : \mathbb{H} \to \mathbb{C}$ is bijective, holom
- $j(it) \in \mathbb{R}$ ($j(z) = \frac{1}{q} + 744 + \cdots \in \mathbb{Z}((q))$ with $q = e^{2\pi i z}$ and $q \in \mathbb{R}$ if $z = it$)
- $j(\mathcal{O}_K) = j(\mathcal{O}_{K'}) \Leftrightarrow K = K'$. (since $j(\Lambda) = j(\Lambda') \Leftrightarrow \Lambda$ and Λ' are homothetic)
- j $SL_2\mathbb{Z}$ invariant.

DEF: $\gamma_2(z) = 12 \dfrac{g_2(z)}{\sqrt[3]{\Delta}(z)}$ (choose $\sqrt[3]{\Delta}$ so that $\sqrt[3]{\Delta}(it) \in \mathbb{R}$)

$\eta(z+1) = \zeta_{24}\, \eta(z)$

$\eta(-\frac{1}{z}) = \sqrt{-iz}\, \eta(z)$

Properties:

- $\gamma_2(z)^3 = j(z)$
- ? $\gamma_2(\begin{pmatrix} a & b \\ c & d \end{pmatrix} z) = \zeta_3^{ac - ab + a^2cd\cdots} \gamma_2(z)$ so not quite $SL_2(\mathbb{Z})$-invariant.

DEF: Let $\eta(z) = q^{1/24} \prod (1 - q^n)$, $q = e^{2\pi i z}$ be the Dedekind eta-function. Then the weber functions are:

$$\mathfrak{f}(z) = \zeta_{48}^{-1} \frac{\eta(\frac{1+z}{2})}{\eta(z)}, \quad \mathfrak{f}_1(z) = \frac{\eta(\frac{z}{2})}{\eta(z)}, \quad \mathfrak{f}_2(z) = \sqrt{2} \frac{\eta(2z)}{\eta(z)}$$

Properties: $\mathfrak{f}_1(2z)\mathfrak{f}_2(z) = \sqrt{2}$ (compare q-series),

$$\begin{cases} \mathfrak{f}(z+1) = \zeta_{48}^{-1} \mathfrak{f}_1(z) & \mathfrak{f}(-1/z) = \mathfrak{f}(z) \\ \mathfrak{f}_1(z+1) = \zeta_{48}^{-1} \mathfrak{f}(z) & \mathfrak{f}_1(-1/z) = \mathfrak{f}_2(z) \\ \mathfrak{f}_2(z+1) = \zeta_{24} \mathfrak{f}_2(z) & \mathfrak{f}_2(-1/z) = \mathfrak{f}_1(z) \end{cases}$$

$$\boxed{\text{THM: } \gamma_2(z) = \frac{\mathfrak{f}(z)^{24} - 16}{\mathfrak{f}(z)^8} = \frac{\mathfrak{f}_1(z)^{24} + 16}{\mathfrak{f}_1(z)^8} = \frac{\mathfrak{f}_2(z)^{24} + 16}{\mathfrak{f}_2(z)^8}}$$

$e_3 - e_1 = \pi^2 \eta(z)^4 \mathfrak{f}_2(z)^8$

Pf: (sketch) $\Delta(z) = 16(e_1-e_2)^2(e_1-e_3)^2(e_2-e_3)^2$ where $e_2 - e_1 = \pi^2 \eta(z)^4 \mathfrak{f}(z)^8$, $e_2 - e_3 = \pi^2 \eta(z)^4 \mathfrak{f}_1(z)^8$

By computing $\wp(\omega) - \wp(\omega')$ in terms of σ_Λ ($\frac{d^2}{dz^2} \log \sigma_\Lambda = -\wp_\Lambda$) which has a q-series comparable to those of $\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2$.

Since e_1, e_2, e_3 are roots of $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$, use Newton-Girard to express $g_2(\Lambda)$ and $g_3(\Lambda)$ in terms of $\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2$.

THM: (Main Theorem of CM) Let $\mathcal{O}$ be an order in an imaginary quadratic field.

i) $j(\mathcal{O})$ is an algebraic integer, $K(j(\mathcal{O}))$ is the <u>ring class field</u> of $\mathcal{O}$, $\mathcal{C}(\mathcal{O}) \cong \mathrm{Gal}(L/K)$.

maximal ~~unique~~ abelian ext. unramified outside of $f\mathcal{O}$.

ii) if $\mathcal{O} = \langle 1, z_0 \rangle$, $z_0 = \begin{cases} \sqrt{D}/4 & D \equiv 0 \pmod 4 \\ \frac{3+\sqrt{D}}{2} & D \not\equiv 0 \pmod 4 \end{cases}$, $3 \nmid D$

$\gamma_2(z_0)$ is an algebraic integer, $K(\gamma_2(z_0)) = L$ is the r.c.f of $\mathcal{O}$ and $\mathcal{C}(\mathcal{O}) \cong \mathrm{Gal}(L/K)$

in fact $\mathbb{Q}(\gamma_2(z_0)) = \mathbb{Q}(j(z_0))$.

iii) if $\mathcal{O} = \langle 1, \sqrt{-m} \rangle$, $3 \nmid m$, $m \equiv 3 \pmod 4$, then $K = \mathbb{Q}(\sqrt{-m})$.

$f(\sqrt{-m})^2$ is an algebraic integer, $\mathcal{C}(\mathcal{O}) \cong \mathrm{Gal}(K(f(\sqrt{-m})^2)/K)$

<u>Pf:</u> really hard. (ii) and (iii) sort of follow from (i) but require heavy use of the transformation laws of γ_2, f, f_1, f_2 and Galois Theory.

The relations given by THM give us a concrete way of computing $j(\mathcal{O})$ when $h(\mathcal{O}) = 1$.

Note that if $h(\mathcal{O}) = 1 \Rightarrow \underset{\gamma_2}{j}(\mathcal{O}) \in \mathbb{Q}$ (since $\underset{\gamma_2}{j}(\mathcal{O})$ is real) $\Rightarrow \underset{\gamma_2}{j}(\mathcal{O}) \in \mathbb{Z}$

In fact:

$m = 1, 2, 4, 7$: $\gamma_2(\sqrt{-m}) = [\![256 q^{2/3} + q^{-1/3}]\!]$

$m = 7, 11, 19, 43, 67, 163$ $\gamma_2\left(\frac{3+\sqrt{-m}}{2}\right) = [\![-q^{-1/6} + 256 q^{1/3}]\!]$ nearest integer.

<u>Pf:</u> (sketch) $f_2(\sqrt{-m}) = \sqrt{2}\, q^{1/24} \prod (1+q^n) \overset{1+x<e^x}{<} \sqrt{2}\, q^{1/24} \prod e^{q^n} = \sqrt{2}\, q^{1/24} e^{\frac{q}{1-q}}$ since $\frac{q}{1-q} < \frac{q}{1-e^{2\pi}} < 1.002q$

$\Rightarrow \sqrt{2}\, q^{1/24} < f_2(\sqrt{-m}) < \sqrt{2}\, q^{1/24} e^{1.002q} \Rightarrow 256 q^{2/3} + q^{-1/3} e^{-8.016q} < \gamma_2(\sqrt{-m}) < e^{16.032} 256 q^{2/3} + q^{-1/3}$

an elementary estimate of the difference of the two ends gives it is <1 so choose any $x = 256q^{2/3} + q^{-1/3}$ in between these bounds.

Using these techniques we have:

d_K	-3	-4	-7	-8	-11	-19	-43	-67	-163
z_0	$\frac{1+\sqrt{-3}}{2}$	i	$\frac{3+\sqrt{-7}}{2}$	$\sqrt{-2}$	$\frac{3+\sqrt{-11}}{2}$	$\frac{3+\sqrt{-19}}{2}$			
$\gamma_2(z_0)$	$-$	12	-15	20	-32	-96	-960	-5280	-640320
$j(z_0)$	0	12^3	-15^3	20^3	-32^3	-96^3	-960^3	-5280^3	-640320^3

well-known

§3. Main Theorem

$d_K = \begin{cases} D & D \equiv 1 \\ 4D & D \not\equiv 1 \end{cases}$

D, $\square$-free

THM: Let K be imaginary quadratic field of discriminant d_K, then $(K = \mathbb{Q}(\sqrt{D}))$

$$h(d_K) = 1 \iff d_K \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$$

Pf:

($\Leftarrow$) Compute all reduced forms of discriminant ~~$D = f^2 d_K$~~ d_K (recall the calculation of $h(-12)$).

($\Rightarrow$)

① Reduction to case $-p = d_K$, $p \equiv 3 \pmod 8$.

we know that $d_K \equiv 0, 1 \pmod 4$.

case 1| $d_K \equiv 0 \pmod 4$, then $d_K = -4n$, $n > 0$. By $\boxed{\text{Landau}}$, $n \in \{1, 2, 3, 4, 7\}$ so $d_K \in \{-4, -8, \cancel{-12}, \cancel{-16}, \cancel{-28}\}$, but $d_K/4$ has to be $\square$-free and $d_K/4 \not\equiv 1 \pmod 4$

$\Rightarrow d_K \in \{-4, -8\}$ ✓

case 2| $d_K \equiv 1 \pmod 4$. By the $\boxed{\text{2-torsion of } C(d_K)}$, $2^{r-1} \leq h(d_K) = 1 \Rightarrow r = 1$ where $r = \#$ prime divisors of d_K. Thus $d_K = -p$ for p prime and $p \equiv 3 \pmod 4$.

case 2.1| $p \equiv 7 \pmod 8$, by the $\boxed{\text{class number formula}}$,

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

Again by $\boxed{\text{Landau}}$ $p \in \{\cancel{1}, \cancel{2}, 3, \cancel{4}, 7\}$, i.e. $p = 7$ ($p \neq 7$) $\Rightarrow d_K = -7$.

② Case when $d_K = -p$, p prime, $p \equiv 3 \pmod 8$.

- By the $\boxed{\text{class number formula}}$, $h(-4p) = 2h(-p)\left(1 - \underbrace{\left(\tfrac{-p}{2}\right)}_{=-1}\tfrac{1}{2}\right) = 3$
- $K = \mathbb{Q}(\sqrt{-p})$, $\mathcal{O}_K = \langle 1, \frac{3+\sqrt{-p}}{2} \rangle$. choose $\mathcal{O} = \langle 1, \sqrt{-p} \rangle$ which has conductor 2 so $D = +2^2 d_K = -4p$. $\Rightarrow$ $h(-4p) = h(\mathcal{O})$ so $j(\sqrt{-p}) = j(\mathcal{O})$
- By the $\boxed{\text{theory of CM}}$, $[K(j(\sqrt{-p})) : K] = 3$. Since $j(\sqrt{-p}) \in \mathbb{R} \Rightarrow$ $[\mathbb{Q}(j(\sqrt{-p})) : \mathbb{Q}] = 3$.

* By $\boxed{CM}$ and the uniqueness of the ring class field $K(\mathfrak{f}(\sqrt{-p})^2) = K(j(\sqrt{-p}))$

Thus, since $\mathfrak{f}(\sqrt{-p})^2 \in \mathbb{R}$ (use its q-series) then $[\mathbb{Q}(\mathfrak{f}(\sqrt{-p})^2) : \mathbb{Q}] = 3$.

* Set $z_0 = \frac{3+\sqrt{-p}}{2}$, $x = \zeta_8^{-1}\mathfrak{f}_2(z_0)^2$ by the $\boxed{\text{transformation laws of } \mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2}$ and $\boxed{\mathfrak{f}_2(z)\mathfrak{f}_1(2z) = \sqrt{2}}$ then $\alpha = \frac{2}{\mathfrak{f}(\sqrt{-p})^2} \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

Observe that $\alpha \in \mathbb{R}$ and $[\mathbb{Q}(\alpha):\mathbb{Q}] = 3 \Rightarrow [\mathbb{Q}(\alpha^4):\mathbb{Q}] = 3$ so $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^4)$.

• By the relation $\boxed{\gamma_2(z_0) = \frac{\mathfrak{f}_2^{24}(z_0)+16}{\mathfrak{f}_2(z_0)^8} = \frac{(\alpha^4)^3+16}{\alpha^4}}$, α^4 satisfies: $x^3 - \gamma_2(z_0)x - 16 = 0$

[Notice that (for $d_K \neq -3$) $\underline{\gamma_2(z_0) \text{ is an algebraic integer}}$ and generates the ring class field of $\mathcal{O}_K = \langle 1, z_0 \rangle$ which is trivial since $h(\mathcal{O}_K) = h(d_K) = 1$ by assumption.
Thus $\gamma_2(z_0) \in K \underset{\gamma_2 \text{ real}}{\Rightarrow} \gamma_2(z_0) \in \mathbb{Z}$. $\therefore$ $x^3 - \gamma_2(z_0)x - 16 \in \mathbb{Z}[x]$]

Since $[\mathbb{Q}(\alpha^4):\mathbb{Q}] = 3$ then $x^3 - \gamma_2(z_0)x - 16 = \min_{\alpha^4/\mathbb{Q}}(x)$

· The above implies that α is an alg. integer so if $g(x) = x^3 + ax^2 + bx + c$ is its minimal polynomial $\Rightarrow a, b, c \in \mathbb{Z}$.

If we separate odd and even degree terms and square both sides, we get

$$\alpha^6 + \underbrace{(2b-a^2)}_{e}\alpha^4 + \underbrace{(b^2-2ac)}_{f}\alpha^2 \underbrace{-c^2}_{g} = 0$$

Doing the same but separating the terms α^6, α^2 from α^4, α^0 we get

$$\alpha^{12} + (2f-e^2)\alpha^8 + (f^2-2eg)\alpha^4 - g^2 = 0 \Rightarrow \alpha^4 \text{ satisfies } x^3 + (2f-e^2)x^2 + (f^2-2eg)x - g^2$$

By the uniqueness of the minimal polynomial:

$$\left\{\begin{array}{l} 0 = 2f - e^2 \\ -\gamma_2(z_0) = f^2 - 2eg \\ -16 = -g^2 \end{array}\right\} \rightarrow g = \pm 4 \Rightarrow c = \pm 2 \quad \text{w.l.o.g. } c = 2$$

swap $\alpha, -\alpha$.

$$\hookrightarrow \left\{\begin{array}{l} 2(b^2 - 4a) = (2b-a^2)^2 \\ \gamma_2(z_0) = -(b^2-4a)^2 - 8(2b-a^2) \end{array}\right. \xrightarrow{2|a,\ 2b} X = -\frac{a}{2},\ Y = \frac{b-a^2}{2} \rightsquigarrow 2X(X^3+1) = Y^2$$

$a = -2X$, $b = 4X^2 + 2Y$

• <u>PROP</u>: The diophantine equation $2X(X^3+1) = Y^2$ has only solutions $(0,0), (-1,0), (1,\pm 2), (2,\pm 6)$

<u>Pf</u>: since $\gcd(X, X^3+1) = 1$, then $\pm(X^3+1)$ is a square or twice a square. This gives:

i) $X^3+1 = Z^2$

ii) $X^3+1 = -Z^2$

iii) $X^3+1 = 2Z^2 \rightsquigarrow W^6+1 = 2Z^2$ (since $4XZ^2 = Y^2 \Rightarrow X$ is a $\square$)

iv) $X^3+1 = -2Z^2$

Now the solutions are:

i) $(-1,0), (0,\pm 1), (2,\pm 3)$ (infinite descent, one or <u>elliptic curves</u>)

$\hookrightarrow$ $y^2 = x^3+1$ has rank 0 so we can use Nagel-Lutz since $\{\text{integral points}\} \supseteq E_{tor}$

ii) $(-1,0)$ (work over $\mathbb{Z}[i]$)

iii) $(1,\pm 1)$ (work over $\mathbb{Z}[\zeta_3]$)

iv) $(-1,0)$ (work over $\mathbb{Z}[\sqrt{-2}]$)

e.g. (ii) $X^3+1 = -Z^2 = (\pm iZ)^2 \Rightarrow (X+1)(X^2+X+1) = (iZ)^2$

$\pi | X \Rightarrow \pi / 1!$

Since $\gcd(X+1, X^2-X+1) = 1$ (if $\pi | X+1, X^2-X+1 \Rightarrow \pi | X(X-2) \Rightarrow \pi / X-2 \Rightarrow \pi | -3$

$\Rightarrow \pi = 3$ since 3 is prime in $\mathbb{Z}[i]$

~~but $\pi | X^2-X+1$, $\pi | X+1 \Rightarrow X \equiv -1 \pmod 3 \Rightarrow X^2-X+1$~~

• Thus we compute $\gamma_2(z_0)$ with (X,Y): $a = -2X$, $b = 4X^2+2Y$, $\gamma_2(z_0) = \cdots$

(X,Y)	(a,b)	$\gamma_2(z_0)$	$j(z_0)$		d_K
$(0,0)$	$(0,0)$	0	0	$\rightsquigarrow$	-3
$(-1,0)$	$(2,4)$	-96	-96^3		-19
$(1,2)$	$(-2,8)$	-5280	-5280^3		-67
$(1,-2)$	$(-2,0)$	-32	-32^3		-11
$(2,6)$	$(-4,28)$	-640320	-640320^3		-163
$(2,-6)$	$(-4,4)$	-960	-960^3		-43

which are exactly the <u>j-invariants associated to</u>

since <u>$j(\mathcal{O}_K) = j(\mathcal{O}_{K'}) \Rightarrow K = K'$.</u>