Class groups and units of certain number fields

Jianing Li

University of Science and Technology of China

February 3, 2021 / Xi'AN JIAOTONG - LIVERPOOL UNIVERSITY

Introduction

A complex number is called algebraic if it is a root of some polynomial $f(x) \in \mathbb{Q}[x]$.
Let $\bar{\mathbb{Q}}$ denote the set of all algebraic numbers. It is a subfield of $\mathbb{C}$.

An algebraic number is called an algebraic integer if it is a root of some monic polynomial $f(x) \in \mathbb{Z}[x]$.
Example: $\sqrt{2}$, $\exp(2\pi i/5)$. Non-example: $\frac{1}{2}$, $\frac{\sqrt{2}}{2}$.
Let $\bar{\mathbb{Z}}$ denote the set of all algebraic integers. It is in fact a subring of $\bar{\mathbb{Q}}$.

Let K be a number field, i.e., a finite extension of $\mathbb{Q}$. Let $\mathcal{O}_K = K \cap \bar{\mathbb{Z}}$ be the ring of (algebraic) integers of K.
Such fields and rings occur naturally when solving Diophantine equations.

$K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Equation: $y^2 + 5 = x^3$.
In $\mathcal{O}_K$, LHS $= (y + \sqrt{-5})(y - \sqrt{-5})$.

$K = \mathbb{Q}(\zeta_n)$, $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ where $\zeta_n = \exp(\frac{2\pi i}{n})$ is a primitive root of 1.
Fermat's equation: $x^n + y^n = z^n$ $(n \geq 3)$.
In $\mathcal{O}_K$, LHS $= (x + y)(x + \zeta_n y) \cdots (x + \zeta_n^{n-1} y)$.

Introduction

A complex number is called algebraic if it is a root of some polynomial $f(x) \in \mathbb{Q}[x]$.
Let $\bar{\mathbb{Q}}$ denote the set of all algebraic numbers. It is a subfield of $\mathbb{C}$.

An algebraic number is called an algebraic integer if it is a root of some monic polynomial $f(x) \in \mathbb{Z}[x]$.
Example: $\sqrt{2}$, $\exp(2\pi i/5)$. Non-example: $\frac{1}{2}$, $\frac{\sqrt{2}}{2}$.
Let $\bar{\mathbb{Z}}$ denote the set of all algebraic integers. It is in fact a subring of $\bar{\mathbb{Q}}$.

Let K be a number field, i.e., a finite extension of $\mathbb{Q}$. Let $\mathcal{O}_K = K \cap \bar{\mathbb{Z}}$ be the ring of (algebraic) integers of K.
Such fields and rings occur naturally when solving Diophantine equations.

$K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Equation: $y^2 + 5 = x^3$.
In $\mathcal{O}_K$, LHS $= (y + \sqrt{-5})(y - \sqrt{-5})$.

$K = \mathbb{Q}(\zeta_n)$, $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ where $\zeta_n = \exp(\frac{2\pi i}{n})$ is a primitive root of 1.
Fermat's equation: $x^n + y^n = z^n$ $(n \geq 3)$.
In $\mathcal{O}_K$, LHS $= (x + y)(x + \zeta_n y) \cdots (x + \zeta_n^{n-1} y)$.

Introduction

A complex number is called algebraic if it is a root of some polynomial $f(x) \in \mathbb{Q}[x]$.
Let $\bar{\mathbb{Q}}$ denote the set of all algebraic numbers. It is a subfield of $\mathbb{C}$.

An algebraic number is called an algebraic integer if it is a root of some monic polynomial $f(x) \in \mathbb{Z}[x]$.
Example: $\sqrt{2}$, $\exp(2\pi i/5)$. Non-example: $\frac{1}{2}$, $\frac{\sqrt{2}}{2}$.
Let $\bar{\mathbb{Z}}$ denote the set of all algebraic integers. It is in fact a subring of $\bar{\mathbb{Q}}$.

Let K be a number field, i.e., a finite extension of $\mathbb{Q}$. Let $\mathcal{O}_K = K \cap \bar{\mathbb{Z}}$ be the ring of (algebraic) integers of K.
Such fields and rings occur naturally when solving Diophantine equations.

$K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Equation: $y^2 + 5 = x^3$.
In $\mathcal{O}_K$, LHS $= (y + \sqrt{-5})(y - \sqrt{-5})$.

$K = \mathbb{Q}(\zeta_n)$, $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ where $\zeta_n = \exp(\frac{2\pi i}{n})$ is a primitive root of 1.
Fermat's equation: $x^n + y^n = z^n$ ($n \geq 3$).
In $\mathcal{O}_K$, LHS $= (x + y)(x + \zeta_n y) \cdots (x + \zeta_n^{n-1} y)$.

Introduction

A complex number is called algebraic if it is a root of some polynomial $f(x) \in \mathbb{Q}[x]$.
Let $\bar{\mathbb{Q}}$ denote the set of all algebraic numbers. It is a subfield of $\mathbb{C}$.

An algebraic number is called an algebraic integer if it is a root of some monic polynomial $f(x) \in \mathbb{Z}[x]$.
Example: $\sqrt{2}$, $\exp(2\pi i/5)$. Non-example: $\frac{1}{2}$, $\frac{\sqrt{2}}{2}$.
Let $\bar{\mathbb{Z}}$ denote the set of all algebraic integers. It is in fact a subring of $\bar{\mathbb{Q}}$.

Let K be a number field, i.e., a finite extension of $\mathbb{Q}$. Let $\mathcal{O}_K = K \cap \bar{\mathbb{Z}}$ be the ring of (algebraic) integers of K.
Such fields and rings occur naturally when solving Diophantine equations.

$K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Equation: $y^2 + 5 = x^3$.
In $\mathcal{O}_K$, LHS $= (y + \sqrt{-5})(y - \sqrt{-5})$.

$K = \mathbb{Q}(\zeta_n)$, $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ where $\zeta_n = \exp(\frac{2\pi i}{n})$ is a primitive root of 1.
Fermat's equation: $x^n + y^n = z^n$ $(n \geq 3)$.
In $\mathcal{O}_K$, LHS $= (x + y)(x + \zeta_n y) \cdots (x + \zeta_n^{n-1} y)$.

Introduction

The ring $\mathcal{O}_K$ does not have unique factorization in general. For example, in $\mathbb{Z}[\sqrt{-5}]$

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

But every nonzero ideal of $\mathcal{O}_K$ can be written as a product of prime ideals uniquely. For example

$$(6) = (2, 1 + \sqrt{-5})^2(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

None of the three ideals on the right is principal.

How to measure the obstruction from the ring $\mathcal{O}_K$ to a principal ideal domain?

Introduction

The ring $\mathcal{O}_K$ does not have unique factorization in general. For example, in $\mathbb{Z}[\sqrt{-5}]$

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

But every nonzero ideal of $\mathcal{O}_K$ can be written as a product of prime ideals uniquely. For example

$$(6) = (2, 1 + \sqrt{-5})^2 (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

None of the three ideals on the right is principal.

How to measure the obstruction from the ring $\mathcal{O}_K$ to a principal ideal domain?

Class groups

An $\mathcal{O}_K$-submodule J of K is called a **fraction ideal** if $\alpha J \subset \mathcal{O}_K$ is an ideal for some $\alpha \in \mathcal{O}_K \setminus \{0\}$. Put

$$I_K = \{ \text{ all nonzero fractional ideals of } K \}$$

$$P_K = \{ \text{ all nonzero principal fractional ideals of } K \}.$$

Dedekind proved $I_K \cong \oplus_{\mathfrak{p}} \mathfrak{p}^{\mathbb{Z}}$. That is, I_K is a free abelian group whose bases are the prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$.

The **(ideal) class group** of K is defined as $\mathrm{Cl}_K := I_K / P_K$

We have an exact sequence:

$$1 \to \mathcal{O}_K^\times \to K^\times \xrightarrow{i} I_K \to \mathrm{Cl}_K \to 1$$

$$i : \alpha \mapsto (\alpha)$$

The class group Cl_K and the unit group $\mathcal{O}_K^\times$ are two important invariants of K.

Class groups

An $\mathcal{O}_K$-submodule J of K is called a **fraction ideal** if $\alpha J \subset \mathcal{O}_K$ is an ideal for some $\alpha \in \mathcal{O}_K \setminus \{0\}$. Put

$$I_K = \{ \text{ all nonzero fractional ideals of } K\}$$

$$P_K = \{ \text{ all nonzero principal fractional ideals of } K\}.$$

Dedekind proved $I_K \cong \oplus_{\mathfrak{p}} \mathfrak{p}^{\mathbb{Z}}$. That is, I_K is a free abelian group whose bases are the prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$.

The **(ideal) class group** of K is defined as $\mathrm{Cl}_K := I_K / P_K$

We have an exact sequence:

$$1 \to \mathcal{O}_K^\times \to K^\times \xrightarrow{i} I_K \to \mathrm{Cl}_K \to 1$$

$$i : \alpha \mapsto (\alpha)$$

The class group Cl_K and the unit group $\mathcal{O}_K^\times$ are two important invariants of K.

Fundamental theorems

Theorem (Dedekind)

Cl_K is finite for any number field K.

$\#\mathrm{Cl}_K$ is called the **class number** of K, and is usually denoted by h_K. We have $h_K = 1$ if and only if $\mathcal{O}_K$ is a principal ideal domain.

Theorem (Dirichlet)

$\mathcal{O}_K^\times \simeq \mathbb{Z}^{r_1+r_2-1} \times \mathbb{Z}/w\mathbb{Z}$ for some integer d. Here r_1 is the number of real embeddings of K and r_2 is the number of pairs of complex embeddings.

If $K = \mathbb{Q}(\alpha)$ with $f(x) \in \mathbb{Q}[x]$ being the minimal polynomial of α. Then r_1 is the number of real roots of $f(x)$ and r_2 is the number of pairs of non-real roots of $f(x)$.

Example: If $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}_{>0}$ square-free, then $r_1 = 2$ and $r_2 = 0$. We have $\mathcal{O}_K^\times = \varepsilon^{\mathbb{Z}} \times \{\pm 1\}$ for some ε.

If $K = \mathbb{Q}(\sqrt{-d})$ with $d \in \mathbb{Z}_{>0}$ square-free, then $r_1 = 0$ and $r_2 = 1$. Hence $\#\mathcal{O}_K^\times$ is finite.

Fundamental theorems

Theorem (Dedekind)

Cl_K is finite for any number field K.

$\#\mathrm{Cl}_K$ is called the **class number** of K, and is usually denoted by h_K. We have $h_K = 1$ if and only if $\mathcal{O}_K$ is a principal ideal domain.

Theorem (Dirichlet)

$\mathcal{O}_K^\times \simeq \mathbb{Z}^{r_1+r_2-1} \times \mathbb{Z}/w\mathbb{Z}$ for some integer d. Here r_1 is the number of real embeddings of K and r_2 is the number of pairs of complex embeddings.

If $K = \mathbb{Q}(\alpha)$ with $f(x) \in \mathbb{Q}[x]$ being the minimal polynomial of α. Then r_1 is the number of real roots of $f(x)$ and r_2 is the number of pairs of non-real roots of $f(x)$.

Example: If $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}_{>0}$ square-free, then $r_1 = 2$ and $r_2 = 0$. We have $\mathcal{O}_K^\times = \varepsilon^{\mathbb{Z}} \times \{\pm 1\}$ for some ε.

If $K = \mathbb{Q}(\sqrt{-d})$ with $d \in \mathbb{Z}_{>0}$ square-free, then $r_1 = 0$ and $r_2 = 1$. Hence $\#\mathcal{O}_K^\times$ is finite.

More examples

Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathrm{Cl}_K \cong \mathbb{Z}/2\mathbb{Z}$ and $\mathcal{O}_K^\times = \{\pm 1\}$.

Using this, it is not hard to derive that $y^2 + 5 = x^3$ has no $\mathbb{Z}$-solutions.

Let $K = \mathbb{Q}(\sqrt{223})$. Then $\mathrm{Cl}_K \cong \mathbb{Z}/3\mathbb{Z}$ and $\mathcal{O}_K^\times = (224 + 15\sqrt{223})^{\mathbb{Z}} \times \{\pm 1\}$.

$x^2 - 223y^2 = -3$ has a $\mathbb{Q}$-solutions $x = 14/3$, $y = 1/3$, but does not have $\mathbb{Z}$-solutions. In fact, there exist infinitely many primes p such that $x^2 - 223y^2 = \pm p$ has $\mathbb{Q}$-solutions but does not have $\mathbb{Z}$-solutions. The reason behind is $h_K = 3$.

Before Wiles' complete proof of Fermat's last theorem, the best result is due to Kummer which says that, if an odd prime p does not divide the class number of $\mathbb{Q}(\zeta_p)$, then $x^p + y^p = z^p$ does not have nonzero $\mathbb{Z}$-solutions. Primes with this property are called regular primes. The first irregular prime is 37. We have $\mathrm{Cl}_{\mathbb{Q}(\zeta_{37})} \cong \mathbb{Z}/37\mathbb{Z}$. Furthermore,

$$\text{the 37-Sylow subgroup of } \mathrm{Cl}_{\mathbb{Q}(\zeta_{37^n})} \cong \mathbb{Z}/37^n\mathbb{Z} \quad \text{for each } n \geq 1$$

Open problems

Conjecture (Gauss)

There exists infinitely many square free positive integers d such that the class number of $\mathbb{Q}(\sqrt{d})$ is 1.

Conjecture (Weber class number problem)

The class numbers of $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}_2 = \mathbb{Q}(\sqrt{\sqrt{2}+2})$, $\mathbb{Q}_3 = \mathbb{Q}(\sqrt{\sqrt{\sqrt{2}+2}+2})$, $\cdots$ are all 1.

Write $\mathbb{Q}_\infty = \cup \mathbb{Q}_n$. Then $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_2$ and $\mathbb{Q}_n$ is the unique subfield of $\mathbb{Q}_\infty$ of degree 2^n. Here $\mathbb{Z}_2$ is the ring of 2-adic integers. Nowadays, it is conjectured that, for every prime number p, the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ has class number 1.

$$
\begin{tikzcd}
\mathbb{Q}_\infty = \cup \mathbb{Q}_n \arrow[d, dash] \\
\mathbb{Q}_n = \mathbb{Q}(\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}) \arrow[d, dash, "\mathbb{Z}/2^n\mathbb{Z}"] \\
\mathbb{Q}_0 = \mathbb{Q} \arrow[uu, dash, bend left=60, "\mathbb{Z}_2"]
\end{tikzcd}
$$

An example of Iwasawa's theory

In 1950s, Iwasawa studied the p-class numbers of fields in the cyclotomic $\mathbb{Z}_p$-towers $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \subset \mathbb{Q}(\zeta_{p^\infty})$. This forms a $\mathbb{Z}_p$-extension.

Theorem (Iwasawa-Ferrero-Washington)

Let h_n denote the class number of $\mathbb{Q}(\zeta_{p^n})$. Let $e_n \geq 0$ such that p^{e_n} exactly divides h_n. Then there exists two integers $\lambda, \nu \geq 0$ such that, for sufficiently large n,

$$e_n = \lambda n + \nu.$$

Example: If $p = 37$, then $\lambda = 1$ and $\nu = 0$.

Class groups of Kummer towers

Let p and q be two distinct prime numbers.
Let $K_{n,m} = \mathbb{Q}(\sqrt[p^n]{q}, \zeta_{2p^m})$. Then $\mathrm{Gal}(K_{\infty,\infty}/K) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$, where $K_{\infty,\infty} = \cup K_{n,m}$.
Let $h_{n,m}$ denote the class number of $K_{n,m}$. Let $A_{n,m}$ denote the p-Sylow subgroup of the class group of $K_{n,m}$.

Theorem (L-Ouyang-Xu-Zhang 2019)

(1)Assume p is an odd regular prime. If q is a primitive root moduluo p^2, then $p \nmid h_{n,m}$ for $n, m \geq 0$.

(2)Assume $p = 2$.
If $q \equiv 3 \mod 8$, then $h_{n,m}$ is odd for $n, m \geq 0$.
If $q \equiv 5 \mod 8$, then $h_{n,0}$ and $h_{1,m}$ are odd for $n, m \geq 0$, and $2 \parallel h_{n,m}$ for $n \geq 2$ and $m \geq 1$.
If $q \equiv 7 \mod 16$, then $A_{n,0} \cong \mathbb{Z}/2\mathbb{Z}$ and $A_{n,1} \cong (\mathbb{Z}/2\mathbb{Z})^2$ for $n \geq 2$.

Remarks:
(1) Gauss' genus theory implies that 2 does not divides $h_{1,0} = h_{\mathbb{Q}(\sqrt{q})}$;
(2) Parry in 1980s studied the 2-divisibility of $h_{2,0} = h_{\mathbb{Q}(\sqrt[4]{q})}$;
(3) It seems that the class number of $K_{n,0} = \mathbb{Q}(\sqrt[2^n]{q})$ is not studied before, even for a single $n \geq 3$.

Units and p-adic regulators

Let $q \equiv 7 \mod 16$ be a prime so that 2 splits in K. Let η be a fundamental unit of F, so that $\mathcal{O}_F^\times = \eta^{\mathbb{Z}} \times \{\pm 1\}$.

$$\begin{array}{ccc} F = \mathbb{Q}(\sqrt[4]{-q}) & w & & w^* \\ | & | & & | \\ K = \mathbb{Q}(\sqrt{-q}) & \mathfrak{p} & & \mathfrak{p}^* \\ | & & \diagdown \quad \diagup & \\ \mathbb{Q} & & 2 & \end{array}$$

By properly choosing the fundamental unit η, the following power series converges in the local field F_w and it is called the w-**adic regulator** of F.

$$\log_w(\eta) := \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n}(\eta - 1)^n \in F_w.$$

Similarly, we can define the w^*-adic regulator of F.

Theorem (Coates-L-Li 2020)

Assume $q \equiv 7 \mod 16$ is a prime. We assume w is ramified in F/K. Then, if η is a fundamental unit of F, we have

$$\mathrm{ord}_w(\log_w(\eta)) = 2, \ \ \mathrm{ord}_{w^*}(\log_{w^*}(\eta)) = 3.$$

Class field theory

Theorem

Let H be the maximal unramified abelian extension of K. Then there is a canonical isomorphism

$$\mathrm{Cl}_K \cong \mathrm{Gal}(H/K).$$

H is called the Hilbert class field of K.

Example: The Hilbert class field of $\mathbb{Q}(\sqrt{-5})$ is $\mathbb{Q}(\sqrt{-5}, \sqrt{-1})$.

A cohomology interpretation of class groups

$$\mathrm{Cl}_K \cong \mathrm{Ker}\, H^1(G_K, \bar{\mathbb{Z}}^\times) \to \prod_v H^1(G_v, \bar{\mathcal{O}}_v^\times).$$

Arithmetic of certain elliptic curves

Assume $q \equiv 7 \mod 16$ is a prime. Let H be the Hilbert class field of $K = \mathbb{Q}(\sqrt{-q})$.
(Gross) There is an elliptic curve A defined over H, with complex multiplication by $\mathcal{O}_K$, minimal discriminant $(-q^3)$, and which is a $\mathbb{Q}$-curve in the sense that it is isogenous to all of its conjugates. Let $B = \mathrm{Res}_K^H A$. Then B is an h_K-dimensional abelian variety defined over K. We have $B(K) \cong A(H)$ as abelian groups.

Example

If $q = 7$, then A is defined by the Weierstrass equation $y^2 + xy = x^3 - x^2 - 2x - 1$ and we have $B = A$ as $h_K = 1$.

Theorem (Coates-L-Li 2020)

Let K_∞ be the unique $\mathbb{Z}_2$-extension of K unramified outside $\mathfrak{p}$. Let $D = K(\sqrt{-1})$ and $D_\infty = DK_\infty$. Let $J = DF = \mathbb{Q}(\sqrt[4]{-q}, \sqrt{-1})$. Assume $q \equiv 7 \mod 16$ is a prime. Then $\dim_{\mathbb{Q}} B(K_\infty) \otimes \mathbb{Q} = 0$ and

$$\dim_{\mathbb{Q}} B(D) \otimes \mathbb{Q} = \dim_{\mathbb{Q}} B(D_\infty) = \dim_{\mathbb{Q}} B(J) \otimes \mathbb{Q} = \dim_{\mathbb{Q}} B(J_\infty) \otimes \mathbb{Q} = 2h_K.$$

The proof of this theorem heavily relies on our results on units of $F = \mathbb{Q}(\sqrt[4]{-q})$.

Arithmetic of certain elliptic curves

Assume $q \equiv 7 \mod 16$ is a prime. Let H be the Hilbert class field of $K = \mathbb{Q}(\sqrt{-q})$.
(Gross) There is an elliptic curve A defined over H, with complex multiplication by $\mathcal{O}_K$, minimal discriminant $(-q^3)$, and which is a $\mathbb{Q}$-curve in the sense that it is isogenous to all of its conjugates. Let $B = \mathrm{Res}_K^H A$. Then B is an h_K-dimensional abelian variety defined over K. We have $B(K) \cong A(H)$ as abelian groups.

Example

If $q = 7$, then A is defined by the Weierstrass equation $y^2 + xy = x^3 - x^2 - 2x - 1$ and we have $B = A$ as $h_K = 1$.

Theorem (Coates-L-Li 2020)

Let K_∞ be the unique $\mathbb{Z}_2$-extension of K unramified outside $\mathfrak{p}$. Let $D = K(\sqrt{-1})$ and $D_\infty = DK_\infty$. Let $J = DF = \mathbb{Q}(\sqrt[4]{-q}, \sqrt{-1})$. Assume $q \equiv 7 \mod 16$ is a prime. Then $\dim_{\mathbb{Q}} B(K_\infty) \otimes \mathbb{Q} = 0$ and

$$\dim_{\mathbb{Q}} B(D) \otimes \mathbb{Q} = \dim_{\mathbb{Q}} B(D_\infty) = \dim_{\mathbb{Q}} B(J) \otimes \mathbb{Q} = \dim_{\mathbb{Q}} B(J_\infty) \otimes \mathbb{Q} = 2h_K.$$

The proof of this theorem heavily relies on our results on units of $F = \mathbb{Q}(\sqrt[4]{-q})$.

The Tate-Shafarevich group

The Tate-Shafarevich group of B/L is defined by

$$Ш(B/L) = \mathrm{Ker} \quad (H^1(\mathrm{Gal}(\bar{L}/L), B(\bar{L})) \to \prod_v H^1(\mathrm{Gal}(\bar{L}_v/L_v), B(\bar{L}_v))),$$

Theorem (Coates-L-Li 2020)

Assume $q \equiv 7 \mod 16$ is a prime. Then $Ш(B/D_\infty)(\mathfrak{P}) = 0$ where $\mathfrak{P}$ is a certain prime of the complex multiplication ring of B lying above 2.

Questions and Remarks

Thanks for your attention!