Vol. 42 (2022)
No. 2

数 学 杂 志
J. of Math. (PRC)

ON $\mathbb{F}_p$-ROOTS OF THE HILBERT CLASS POLYNOMIAL MODULO p

CHEN Ming-jie[1], XUE Jiang-wei[2]

(1. *Department of Mathematics, University of California San Diego, 9500 Gilman Drive,
La Jolla, CA 92093-0112*)

(2. *School of Mathematics and Statistics, Collaborative Innovation Center of Mathematics,
Wuhan University, Hubei Key Laboratory of Computational Science,
Wuhan 430072, China)*

Abstract: The Hilbert class polynomial $H_{\mathcal{O}}(x) \in \mathbb{Z}[x]$ attached to an order $\mathcal{O}$ in an imaginary quadratic field K is the monic polynomial whose roots are precisely the distinct j-invariants of elliptic curves over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$. Let p be a prime inert in K and strictly greater than $|\operatorname{disc}(\mathcal{O})|$. We show that the number of $\mathbb{F}_p$-roots of $H_{\mathcal{O}}(x) \pmod p$ is either zero or $|\operatorname{Pic}(\mathcal{O})[2]|$ by exhibiting a free and transitive action of $\operatorname{Pic}(\mathcal{O})[2]$ on the set of $\mathbb{F}_p$-roots of $H_{\mathcal{O}}(x) \pmod p$ whenever it is nonempty. We also provide a concrete criterion for the existence of $\mathbb{F}_p$-roots. A similar result was first obtained by Xiao et al. [25] and generalized much further by Li et al. [13] (that covers the current result) with a different approach.

Keywords: Hilbert class polynomial; supersingular elliptic curve; endomorphism ring; quaternion algebra, Picard group.

2010 MR Subject Classification: 14H52; 11G20; 11R52; 11G15

Document code: A **Article ID:** 0255-7797(2022)02-0108-13

1 Introduction

Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and $\operatorname{Pic}(\mathcal{O})$ be the Picard group of $\mathcal{O}$, i.e. the group of isomorphism classes of invertible fractional $\mathcal{O}$-ideals under multiplication. The Hilbert class polynomial $H_{\mathcal{O}}(x)$ attached to $\mathcal{O}$ is defined to be

$$H_{\mathcal{O}}(x) = \prod_{[\mathfrak{a}] \in \operatorname{Pic}(\mathcal{O})} (x - \mathfrak{j}(\mathbb{C}/\mathfrak{a})), \tag{1.1}$$

where $[\mathfrak{a}]$ denotes the isomorphism class of the invertible fractional $\mathcal{O}$-ideal $\mathfrak{a}$, and $\mathfrak{j}(\mathbb{C}/\mathfrak{a})$ stands for the $\mathfrak{j}$-invariant of the complex elliptic curve $\mathbb{C}/\mathfrak{a}$. It is well known that $H_{\mathcal{O}}(x)$ has integral coefficients, and it is irreducible over $\mathbb{Q}$ (see [3, §13] and [12, Chapter 10, App., p.144]).

Let $p \in \mathbb{N}$ be a prime number, and $\widetilde{H}_{\mathcal{O}}(x) \in \mathbb{F}_p[x]$ be the polynomial obtained by reducing $H_{\mathcal{O}}(x) \in \mathbb{Z}[x]$ modulo p. Suppose that p is non-split in K so that the roots of

* **Received date:** 2021-02-18 **Accepted date:** 2021-03-14
Foundation item: Supported by NSF grants DMS-1844206, DMS-1802161.

$\widetilde{H}_{\mathcal{O}}(x)$ are supersingular j-invariants, which are known to lie in $\mathbb{F}_{p^2}$. It's natural to ask how many of them are actually in $\mathbb{F}_p$. Castryck, Panny, and Vercauteren answered this question in [4, Theorem 26] for special cases when $p \equiv 3 \pmod 4$, K is of the form $\mathbb{Q}(\sqrt{-l})$ with l prime, $l < (p+1)/4$ and $\mathcal{O}$ is an order containing $\sqrt{-l}$. Their method as in [4, Section 5.2] counts the $\mathbb{F}_p$-roots by constructing supersingular elliptic curves over $\mathbb{F}_p$. We take a different approach here by reinterpreting the $\mathbb{F}_p$-roots in terms of quaternion orders, which allows us to answer the question in more generality.

Our main result is as follows.

Theorem 1.1 Let K be an imaginary quadratic field and $\mathcal{O}$ be an order in K. Let p be a prime inert in K and strictly greater than $|\operatorname{disc}(\mathcal{O})|$, and $\mathcal{H}_p$ be set of $\mathbb{F}_p$-roots of $\widetilde{H}_{\mathcal{O}}(x)$. If $\mathcal{H}_p$ is nonempty, then it admits a regular (i.e. free and transitive) action by the 2-torsion subgroup $\operatorname{Pic}(\mathcal{O})[2] \subset \operatorname{Pic}(\mathcal{O})$. In particular, the number of $\mathbb{F}_p$-roots of $\widetilde{H}_{\mathcal{O}}(x)$ is either zero or $|\operatorname{Pic}(\mathcal{O})[2]|$.

Moreover, $\mathcal{H}_p \neq \emptyset$ if and only if for every prime factor ℓ of $\operatorname{disc}(\mathcal{O})$, either condition (i) or (ii) below holds for ℓ depending on its parity:

(i) $\ell \neq 2$ and the Legendre symbol $\left(\frac{-p}{\ell}\right) = 1$;

(ii) $\ell = 2$ and one of the following conditions holds:

(a) $p \equiv 7 \pmod 8$;

(b) $-p + \frac{\operatorname{disc}(\mathcal{O})}{4} \equiv 0$, 1 or $4 \pmod 8$;

(c) $-p + \operatorname{disc}(\mathcal{O}) \equiv 1 \pmod 8$.

The assumption that $|\operatorname{disc}(\mathcal{O})| < p$ immediately implies that p does not divide the discriminant of $H_{\mathcal{O}}(x)$ by an influential work of Gross and Zagier [8]. Therefore, $\widetilde{H}_{\mathcal{O}}(x)$ has no repeated roots. We provide an alternative proof of this fact under the current assumptions in Corollary 2.7.

Remark 1.2 After the first of version of this manuscript appeared on the web, Jianing Li kindly informed us that a similar result to Theorem 1.1 has firstly been obtained in [25, Theorem 1.1] under the assumption that $|\operatorname{disc}(\mathcal{O})| < 4\sqrt{p/3}$. Moreover, Li et al. used a method similar to [25] and generalized it much further in a joint work [13]. Their result is as follows. Let $\mathrm{j}_0 = \mathrm{j}(\mathbb{C}/\mathcal{O})$, and put $L := \mathbb{Q}(\mathrm{j}_0)$. If p coprime to the index $[\mathcal{O}_L : \mathbb{Z}[\mathrm{j}_0]]$ (e.g. if $p \nmid \operatorname{disc}(\mathcal{O})$), then they completely determined the factorization of $\widetilde{H}_{\mathcal{O}}(x)$ in $\mathbb{F}_p[x]$. Partial results are also obtained without the co-primality condition. In particular, the results of Theorem 1.1 has been covered in [13, Theorem 4.1]. On the other hand, the current project was initiated in May 2021 during an online discussion between the authors. Unaware of the significant progress made by aforementioned works, we worked independently and obtained Theorem 1.1 by a completely different method: we count the $\mathbb{F}_p$-roots by demonstrating a regular action using quaternion orders, whereas the aforementioned works count by studying the factorization of p in L.

For the reader's convenience, we reproduce the celebrated formula of Gauss on the order of $\mathrm{Pic}(\mathcal{O})[2]$.

Theorem 1.3 [3, Proposition 3.11] Let r be the number of odd primes dividing $\mathrm{disc}(\mathcal{O})$. Define the number μ as follows: if $\mathrm{disc}(\mathcal{O}) \equiv 1 \pmod 4$, then $\mu = r$, and if $\mathrm{disc}(\mathcal{O}) \equiv 0 \pmod 4$, then $\mathrm{disc}(\mathcal{O}) = -4n$, where $n > 0$, and μ is determined as follows:

$$\mu = \begin{cases} r & \text{if } n \equiv 3 \pmod 4; \\ r+1 & \text{if } n \equiv 1, 2 \pmod 4; \\ r+1 & \text{if } n \equiv 4 \pmod 8; \\ r+2 & \text{if } n \equiv 0 \pmod 8. \end{cases}$$

Then $|\mathrm{Pic}(\mathcal{O})[2]| = 2^{\mu-1}$.

This paper is organized as follows. In section 2, we give a reinterpretation of $\mathcal{H}_p$ in terms of quaternion orders. In section 3, we show that there is a regular action of $\mathrm{Pic}(\mathcal{O})[2]$ on $\mathcal{H}_p$ whenever $\mathcal{H}_p \neq \emptyset$, and provide a nonemptiness criterion for $\mathcal{H}_p$. Throughout the paper, the prime $p \in \mathbb{N}$ is assumed to be non-split in K. The notation $B_{p,\infty}$ is reserved for the unique quaternion $\mathbb{Q}$-algebra ramified precisely at p and infinity. Given a set X and an equivalence relation on X, the equivalence class of an element $x \in X$ is denoted by $[x]$.

Acknowledgements The first author would like to thank WIN5 research group members Sarah Arpin, Kristin Lauter, Renate Scheidler, Katherine Stange and Ha Tran for helpful comments on some initial ideas on this problem. The first author would also like to thank Kiran Kedlaya and Rachel Pries for helpful suggestions, and Nandagopal Ramachandran for helpful discussions. The second author thanks Chia-Fu Yu for helpful discussions.

2 Reinterpretation of the $\mathbb{F}_p$-roots

As mentioned before, we are going to reinterpret the $\mathbb{F}_p$-roots of $\widetilde{H}_{\mathcal{O}}(x)$ in terms of quaternion orders. For this purpose, we first describe more concretely the reduction of singular moduli with complex multiplication by $\mathcal{O}$. Assume that the prime p is non-split in K. For the moment, we make no assumption on the discriminant of the order $\mathcal{O} \subset K$.

Let $\mathcal{E}\ell\ell(\mathcal{O})$ be the set of isomorphism classes of elliptic curves over $\overline{\mathbb{Q}}$ with complex multiplication by $\mathcal{O}$. It is canonically identified with the singular j-invariants with complex multiplication by $\mathcal{O}$ (i.e. the roots of $H_{\mathcal{O}}(x) \in \mathbb{Z}[x]$). The Picard group $\mathrm{Pic}(\mathcal{O})$ acts regularly on $\mathcal{E}\ell\ell(\mathcal{O})$ via $\mathfrak{a}$-transformation [19, §7] and [16, §1]:

$$\mathrm{Pic}(\mathcal{O}) \times \mathcal{E}\ell\ell(\mathcal{O}) \to \mathcal{E}\ell\ell(\mathcal{O}), \qquad ([\mathfrak{a}], E) \mapsto E^{\mathfrak{a}}. \tag{2.1}$$

More concretely, if we pick $\mathfrak{a}$ to be an integral ideal of $\mathcal{O}$ and write $E[\mathfrak{a}]$ for the finite group scheme $\cap_{a\in\mathfrak{a}} E[a]$, then $E^{\mathfrak{a}} = E/E[\mathfrak{a}]$ by [24, Corollary A.4]. Here $E[a] = \ker(E \xrightarrow{a} E)$. See [16, Proposition 1.26] and [24, Appendix] for the functorial characterization of $E^{\mathfrak{a}}$. Alternatively, since $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal, $E^{\mathfrak{a}}$ can also be identified canonically with the Serre tensor construction $\mathfrak{a}^{-1} \otimes_{\mathcal{O}} E$ (see [1, §1] and [2, §1.7.4]). Fix a member $E_0 \in \mathcal{E}\ell\ell(\mathcal{O})$.

The regular action in (2.1) gives rise to a $\mathrm{Pic}(\mathcal{O})$-equivariant bijection $\xi : \mathcal{E}\ell\ell(\mathcal{O}) \to \mathrm{Pic}(\mathcal{O})$ that sends E_0 to the identity element $[\mathcal{O}] \in \mathrm{Pic}(\mathcal{O})$.

Similarly, let $\mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$ be the set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, which is canonically identified with the set of supersingular j-invariants in $\mathbb{F}_{p^2}$. From [20, Theorem V.3.1], an elliptic curve $E/\overline{\mathbb{F}}_p$ is supersingular if and only if its endomorphism algebra $\mathrm{End}^0(E) := \mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion $\mathbb{Q}$-algebra. Assume that this is the case. Then $\mathrm{End}^0(E)$ coincides with the unique quaternion $\mathbb{Q}$-algebra $B_{p,\infty}$ ramified precisely at p and infinity, and $\mathrm{End}(E)$ is a maximal order in $\mathrm{End}^0(E)$ by [24, Theorem 4.2]. For simplicity, put $B := B_{p,\infty}$ and let $\mathrm{Typ}(B)$ be the *type set* of B, that is, the set of isomorphism (i.e. $B^\times$-conjugacy) classes of maximal orders in B. We obtain the following canonical map, which is known to be surjective [23, Corollary 42.2.21]:

$$\rho : \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p} \twoheadrightarrow \mathrm{Typ}(B), \qquad E \mapsto [\mathrm{End}(E)]. \tag{2.2}$$

Let $\mathcal{R}$ be a maximal order in B, and $\mathrm{Cl}(\mathcal{R})$ be its left ideal class set, that is, the set of isomorphism (i.e. right $B^\times$-equivalent) classes of fractional left ideals of $\mathcal{R}$ in B. Given a fractional left ideal I of $\mathcal{R}$, we write $\mathcal{R}_r(I)$ for the right order of I, which is defined as follows:

$$\mathcal{R}_r(I) := \{x \in B \mid Ix \subseteq I\}.$$

Sending a fractional left $\mathcal{R}$-ideal to its right order induces a surjective map

$$\Upsilon : \mathrm{Cl}(\mathcal{R}) \twoheadrightarrow \mathrm{Typ}(B), \qquad [I] \mapsto [\mathcal{R}_r(I)]. \tag{2.3}$$

The Deuring correspondence [23, Corollary 42.3.7] establishes a bijection between $\mathrm{Cl}(\mathcal{R})$ and $\mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$. One direction of this correspondence goes as follows. From the surjectivity of ρ, we may always fix $E_{\mathcal{R}} \in \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$ such that $\mathrm{End}(E_{\mathcal{R}}) = \mathcal{R}$. Then the member of $\mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$ corresponding to a left ideal class $[I] \in \mathrm{Cl}(\mathcal{R})$ is the I-transform $E^I_{\mathcal{R}}$ of $E_{\mathcal{R}}$. If I is chosen to be an integral left ideal of $\mathcal{R}$, then $E^I_{\mathcal{R}}$ can be identified with the quotient $E_{\mathcal{R}}/E_{\mathcal{R}}[I]$ by [24, Corollary A.4] again. From [23, Corollary 42.3.7], we have

$$\mathrm{End}(E^I_{\mathcal{R}}) \simeq \mathcal{R}_r(I). \tag{2.4}$$

Let $\mathfrak{P}$ be a place of $\overline{\mathbb{Q}}$ lying above p, and $r_{\mathfrak{P}} : \mathcal{E}\ell\ell(\mathcal{O}) \to \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$ be the reduction map modulo $\mathfrak{P}$. For each $E \in \mathcal{E}\ell\ell(\mathcal{O})$, we write $\widetilde{E}$ for the reduction of E modulo $\mathfrak{P}$. From [12, §9.2], reducing E_0 modulo $\mathfrak{P}$ gives rise to an embedding $\iota : \mathcal{O} \hookrightarrow \mathcal{R}_0 := \mathrm{End}(\widetilde{E}_0)$. By an abuse of notation, we still write ι for both of the following two induced maps:

$$K \hookrightarrow B \quad \text{and} \quad \mathrm{Pic}(\mathcal{O}) \xrightarrow{[\mathfrak{a}] \mapsto [\mathcal{R}_0 \iota(\mathfrak{a})]} \mathrm{Cl}(\mathcal{R}_0). \tag{2.5}$$

For simplicity, we identify K with its image in B via ι and write $\mathcal{R}_0\mathfrak{a}$ for $\mathcal{R}_0\iota(\mathfrak{a})$.

Now we are ready to give a concrete description of $r_{\mathfrak{P}} : \mathcal{E}\ell\ell(\mathcal{O}) \to \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$.

Proposition 2.1 The reduction map $r_{\mathfrak{P}}$ fits into a commutative diagram as follows:

$$\begin{tikzcd}
\mathcal{E}\ell\ell(\mathcal{O}) \arrow[r, "r_{\mathfrak{P}}"] \arrow[d, leftrightarrow, "\xi"', "\simeq"] & \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p} \arrow[d, leftrightarrow, "\delta"', "\simeq"] \arrow[dr, two heads, "\rho"] & \\
\mathrm{Pic}(\mathcal{O}) \arrow[r, "\iota"] & \mathrm{Cl}(\mathcal{R}_0) \arrow[r, two heads, "\Upsilon"] & \mathrm{Typ}(B).
\end{tikzcd}$$

Here ξ is the $\mathrm{Pic}(\mathcal{O})$-equivariant bijection that sends the fixed member $E_0 \in \mathcal{E}\ell\ell(\mathcal{O})$ to $[\mathcal{O}] \in \mathrm{Pic}(\mathcal{O})$, and δ is the Deuring correspondence obtained by taking $E_{\mathcal{R}_0} = \widetilde{E}_0$.

Proof According to [19, Proposition 15, §11], $\mathfrak{a}$-transforms are preserved under good reductions[1]. This implies that for every $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$, we have

$$\widetilde{E_0^{\mathfrak{a}}} = (\widetilde{E}_0)^{\mathfrak{a}} = (\widetilde{E}_0)^{\mathcal{R}_0\mathfrak{a}},$$

so the left square commutes. The right triangle commutes because of (2.4).

Corollary 2.2 For any $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$, we have $\mathrm{End}(\widetilde{E_0^{\mathfrak{a}}}) \simeq \mathfrak{a}^{-1}\mathcal{R}_0\mathfrak{a}$.

Proof This follows directly from Proposition 2.1 since the right order of $\mathcal{R}_0\mathfrak{a}$ is precisely $\mathfrak{a}^{-1}\mathcal{R}_0\mathfrak{a}$.

Remark 2.3 Let $\mathcal{O}_K$ be the ring of integers of K, and f be the conductor of $\mathcal{O}$ so that $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$. Write $f = p^m f'$ with $p \nmid f'$, and put $\mathcal{O}' := \mathbb{Z} + f'\mathcal{O}_K$. According to [17, Lemma 3.1], $\iota(K) \cap \mathcal{R}_0 = \iota(\mathcal{O}')$. For any invertible fractional ideal $\mathfrak{a}$ of $\mathcal{O}$, we have $\mathcal{R}_0\mathfrak{a} = (\mathcal{R}_0\mathcal{O}')\mathfrak{a} = \mathcal{R}_0(\mathcal{O}'\mathfrak{a})$. It follows that the map $\iota : \mathrm{Pic}(\mathcal{O}) \to \mathrm{CI}(\mathcal{R}_0)$ factors through the following canonical homomorphism

$$\varpi : \mathrm{Pic}(\mathcal{O}) \to \mathrm{Pic}(\mathcal{O}'), \qquad [\mathfrak{a}] \mapsto [\mathcal{O}'\mathfrak{a}].$$

From this, one easily deduces that $\widetilde{H}_{\mathcal{O}}(x) = (\widetilde{H}_{\mathcal{O}'}(x))^{|\ker(\varpi)|}$.

Now assume that $\mathcal{O}$ is maximal at p (i.e. $p \nmid f$). From Remark 2.3, $\iota : \mathcal{O} \to \mathcal{R}_0$ is an optimal embedding of $\mathcal{O}$ into $\mathcal{R}_0$, that is, $\iota(K) \cap \mathcal{R}_0 = \iota(\mathcal{O})$. Given an arbitrary maximal order $\mathcal{R}$ of B, we write $\mathrm{Emb}(\mathcal{O}, \mathcal{R})$ for the set of optimal embeddings of $\mathcal{O}$ into $\mathcal{R}$. The unit group $\mathcal{R}^\times$ acts on $\mathrm{Emb}(\mathcal{O}, \mathcal{R})$ by conjugation, and there are only finitely many orbits. Put $m(\mathcal{O}, \mathcal{R}, \mathcal{R}^\times) := |\mathcal{R}^\times \backslash \mathrm{Emb}(\mathcal{O}, \mathcal{R})|$, the number of $\mathcal{R}^\times$-conjugacy clasess of optimal embeddings from $\mathcal{O}$ into $\mathcal{R}$. We recall below a precise formula by Elkies, Ono and Yang for the cardinality of each fiber of the reduction map $r_{\mathfrak{P}} : \mathcal{E}\ell\ell(\mathcal{O}) \to \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$.

Lemma 2.4 [[7, Lemma 3.3]] Suppose that $\mathcal{O}$ is maximal at p. Then for any member $E \in \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$, we have

$$|r_{\mathfrak{P}}^{-1}(E)| = \varepsilon \cdot m(\mathcal{O}, \mathcal{R}, \mathcal{R}^\times),$$

where $\mathcal{R} = \mathrm{End}(E)$, and $\varepsilon = 1/2$ or 1 according as p is inert or ramified in K.

A priori, [7, Lemma 3.3] is only stated for the maximal order $\mathcal{O}_K$. Nevertheless, the same proof there applies more generally to quadratic orders maximal at p. Alternatively, using

[1] A priori, the statement of [19, Proposition 15, §11] requires that $\mathcal{O} = \mathcal{O}_K$, the maximal order of K. Nevertheless, the result here holds for general $\mathcal{O}$ here since $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal by our assumption.

Proposition 2.1 and the Deuring lifting theorem[2] [12, Theorem 14, §13.5] [8, Proposition 2.7], one easily sees that Lemma 2.4 is equivalent to the following purely arithmetic result, whose independent proof will be left for the interested reader.

Lemma 2.5 Keep $\mathcal{O}$ and ε as in Lemma 2.4. Let $\mathcal{R}$ be a maximal order in B, and $\varphi : \mathcal{O} \hookrightarrow \mathcal{R}$ be an optimal embedding. Denote the induced map $\mathrm{Pic}(\mathcal{O}) \to \mathrm{CI}(\mathcal{R})$ by φ as well. Then for each $[I] \in \mathrm{CI}(\mathcal{R})$, we have

$$|\varphi^{-1}([I])| = \varepsilon \cdot m(\mathcal{O}, \mathcal{R}_r(I), \mathcal{R}_r(I)^\times).$$

We immediately obtain the following corollaries from Lemma 2.4 .

Corollary 2.6 Suppose that $\mathcal{O}$ is maximal at p. The $\mathfrak{j}$-invariant of a supersingluar elliptic curve $E/\overline{\mathbb{F}}_p$ is a root of $\widetilde{H}_{\mathcal{O}}(x)$ if and only if $\mathcal{O}$ can be optimally embedded into $\mathrm{End}(E)$.

This matches well with Corollary 2.2. Indeed, a classical result of Chevalley, Hasse and Noether [9, §4] says that any maximal order of B that contains a copy of $\mathcal{O}$ optimally is isomorphic to $\mathfrak{a}^{-1}\mathcal{R}_0\mathfrak{a}$ for some $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$.

Corollary 2.7 If $p > |\operatorname{disc}(\mathcal{O})|$, then the reduction map $r_{\mathfrak{P}} : \mathcal{E}\ell\ell(\mathcal{O}) \to \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$ is injective. In particular, $\widetilde{H}_{\mathcal{O}}(x)$ has no repeated roots.

We give a simple proof that is independent of the result of Gross and Zagier [8].

Proof Since p does not split in K and is strictly greater than $|\mathrm{disc}(\mathcal{O})|$, it is necessarily inert in K. From Lemma 2.4 , it suffices to show that $|\mathrm{Emb}(\mathcal{O}, \mathcal{R})| \leq 2$ for any maximal order $\mathcal{R}$ in B. Since $p > |\operatorname{disc}(\mathcal{O})|$, Kaneko's inequality [10, Theorem 2'] forces any two optimal embeddings $\varphi, \varphi' : \mathcal{O} \to \mathcal{R}$ to have the same image. On the other hand, φ and φ' share the same image if and only if $\varphi' = \varphi$ or $\bar{\varphi}$, the complex conjugate of φ. The desired inequality $|\mathrm{Emb}(\mathcal{O}, \mathcal{R})| \leq 2$ follows immediately.

Remark 2.8 In another direction, Elkies, Ono and Yang [7, Theorem 1.4] showed that there exists a bound N_p such that the reduction map $r_{\mathfrak{P}} : \mathcal{E}\ell\ell(\mathcal{O}_K) \to \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$ is surjective whenever $|\operatorname{disc}(\mathcal{O}_K)| > N_p$. This bound is first effectivized by Kane [11] conditionally upon the generalized Riemann hypothesis. Liu et al. further improved this bound in [14, Corollary 1.3].

Let us return to the task of interpreting $\mathbb{F}_p$-roots of $\widetilde{H}_{\mathcal{O}}(x) \in \mathbb{F}_p[x]$ in terms of maximal orders in B. For the rest of this section, we keep the additional assumption that $p > |\operatorname{disc}(\mathcal{O})|$. We recall from [6, Proposition 2.4] a classical result on supersingular elliptic curves in characteristic p.

Lemma 2.9 Let $p > 3$ and let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$. Then $\mathfrak{j}(E) \in \mathbb{F}_p$ if and only if there exists $\psi \in \mathrm{End}(E)$ such that $\psi^2 = -p$.

Recall that $\mathcal{H}_p$ denotes the set of $\mathbb{F}_p$-roots of $\widetilde{H}_{\mathcal{O}}(x)$, which can be identified canonically with a subset of $\mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$.

[2] Here the Deuring lifting theorem guarantees that the optimal embedding $\iota : \mathcal{O} \to \mathcal{R}_0$ is "non-special", that is, every optimal embedding $\varphi : \mathcal{O} \to \mathcal{R}$ is realizable as $\mathrm{End}(E) \to \mathrm{End}(\widetilde{E})$ for some $E \in \mathcal{E}\ell\ell(\mathcal{O})$.

Lemma 2.10 The map $\rho : \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p} \to \mathrm{Typ}(B)$ in (2.2) induces a bijection between $\mathcal{H}_p$ and the following subset $\mathcal{T}_p \subseteq \mathrm{Typ}(B)$:

$$\mathcal{T}_p := \{[\mathcal{R}] \in \mathrm{Typ}(B) \mid \mathrm{Emb}(\mathcal{O}, \mathcal{R}) \neq \emptyset, \text{ and } \exists \alpha \in \mathcal{R} \text{ such that } \alpha^2 = -p\}. \tag{2.6}$$

Proof Combining Corollary 2.6 and Lemma 2.9, we see that $\rho(\mathcal{H}_p) = \mathcal{T}_p$. Now it follows from [23, Lemma 42.4.1] that $\rho : \mathcal{H}_p \to \mathcal{T}_p$ is injective, and hence bijective.

We give another characterization of $\mathcal{T}_p$ by presenting the quaternion algebra $B = B_{p,\infty}$ more concretely. Let $d \in \mathbb{N}$ be the unique square-free positive integer such that $K = \mathbb{Q}(\sqrt{-d})$. The assumption that p is inert in K amounts to the equality $\left(\frac{-d}{p}\right) = -1$. Let $\left(\frac{-d,-p}{\mathbb{Q}}\right)$ be the quaternion $\mathbb{Q}$-algebra with standard basis $\{1, i, j, k\}$ such that

$$i^2 = -d, \quad j^2 = -p \quad \text{and} \quad k = ij = -ji. \tag{2.7}$$

We identify $K = \mathbb{Q}(\sqrt{-d})$ with $\mathbb{Q}(i)$, and $\mathcal{O}$ with the corresponding order in $\mathbb{Q}(i)$. Put $\Lambda := \mathcal{O} + j\mathcal{O}$, which is an order (of full rank) in the above quaternion algebra. Consider the following finite set of maximal orders:

$$S^{\mathrm{opt}} := \left\{ \mathscr{R} \subset \left(\frac{-d,-p}{\mathbb{Q}}\right) \mid \mathscr{R} \text{ is a maximal order containing } \Lambda \text{ and } \mathscr{R} \cap \mathbb{Q}(i) = \mathcal{O} \right\}. \tag{2.8}$$

Here the superscript "opt" stands for "$\mathcal{O}$-optimal".

Proposition 2.11 Let $\mathcal{R}$ be a maximal order in B. We have $[\mathcal{R}] \in \mathcal{T}_p$ if and only if $\mathcal{R} \simeq \mathscr{R}$ for some $\mathscr{R} \in S^{\mathrm{opt}}$. In particular, $\mathcal{H}_p \neq \emptyset$ if and only if $\left(\frac{-d,-p}{\mathbb{Q}}\right) \simeq B$ and $S^{\mathrm{opt}} \neq \emptyset$.

Proof Clearly, if $\mathcal{R} \simeq \mathscr{R}$ for some $\mathscr{R} \in S^{\mathrm{opt}}$, then $[\mathcal{R}] \in \mathcal{T}_p$. Conversely, suppose that $[\mathcal{R}] \in \mathcal{T}_p$, that is, $\mathcal{R}$ contains a copy of $\mathcal{O}$ optimally, and there exists $\alpha \in \mathcal{R}$ with $\alpha^2 = -p$. Then $\mathcal{R}\alpha$ is the unique two sided prime ideal of $\mathcal{R}$ lying above p. From [22, Exercise I.4.6], $\mathcal{R}$ is normalized by α, which implies that $\mathcal{O}_\alpha := \alpha\mathcal{O}\alpha^{-1}$ is still a quadratic order optimally embedded in $\mathcal{R}$. If $\mathcal{O}_\alpha \neq \mathcal{O}$, then $|\operatorname{disc}(\mathcal{O})| \geq p$ by Kaneko's inequality [10, Theorem 2'], contradicting to our assumption that $|\operatorname{disc}(\mathcal{O})| < p$. Thus $\mathcal{O}_\alpha = \mathcal{O}$, and conjugation by α induces an automorphism $\sigma \in \mathrm{Aut}(\mathcal{O})$. If σ is the identity, then α lies in the centralizer of $\mathcal{O}$ in B, which is just K. This contradicts to the assumption $|\operatorname{disc}(\mathcal{O})| < p$ again. It follows that σ is the unique nontrivial automorphism of $\mathcal{O}$, i.e. the complex conjugation. We conclude that $\Lambda_{\mathcal{R}} := \mathcal{O} + \alpha\mathcal{O} \subset \mathcal{R}$ is isomorphic to Λ, and $B = \Lambda_{\mathcal{R}} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \Lambda \otimes_{\mathbb{Z}} \mathbb{Q} = \left(\frac{-d,-p}{\mathbb{Q}}\right)$. Consequently, $\mathcal{R}$ is isomorphic to some member of S^{opt}. The last statement follows from the bijection $\mathcal{H}_p \simeq \mathcal{T}_p$ in Lemma 2.10.

Lemma 2.12 The isomorphism $\left(\frac{-d,-p}{\mathbb{Q}}\right) \simeq B$ holds if and only if $\left(\frac{-p}{\ell}\right) = 1$ for every odd prime factor ℓ of d.

Proof For the moment, let ℓ be either a prime number or ∞. Write $(-d, -p)_\ell$ for the Hilbert symbol of $-d$ and $-p$ relative to $\mathbb{Q}_\ell$ (where $\mathbb{Q}_\infty = \mathbb{R}$). From [22, Corollaire II.1.2], $\left(\frac{-d,-p}{\mathbb{Q}}\right)$ is split at ℓ if and only if $(-d, -p)_\ell = 1$. Clearly, $(-d, -p)_\infty = -1$.

Now assume that ℓ is an odd prime. By our assumption, p is an odd prime satisfying $\left(\frac{-d}{p}\right) = -1$. From [18, Theorem 1, §III.1], we easily compute that

$$(-d,-p)_\ell = \begin{cases} 1 & \text{if } \ell \nmid (dp); \\ -1 & \text{if } \ell = p; \\ \left(\frac{-p}{\ell}\right) & \text{if } \ell | d. \end{cases}$$

Therefore, if $\left(\frac{-d,-p}{\mathbb{Q}}\right) \simeq B$, then necessarily $\left(\frac{-p}{\ell}\right) = 1$ for every odd prime factor ℓ of d.

Conversely, if $\left(\frac{-p}{\ell}\right) = 1$ for every odd prime factor ℓ of d, then $(-d,-p)_2 = 1$ by the product formula [18, Theorem 2, §III.2]. Hence this condition is also sufficient for the isomorphism $\left(\frac{-d,-p}{\mathbb{Q}}\right) \simeq B$.

3 The $\mathrm{Pic}(\mathcal{O})[2]$-action on $\mathcal{H}_p$ and the Nonemptiness Criterion

Throughout this section, we assume that p is inert in $K = \mathbb{Q}(\sqrt{-d})$ and strictly greater than $|\operatorname{disc}(\mathcal{O})|$. Assume further that the quaternion $\mathbb{Q}$-algebra $\left(\frac{-d,-p}{\mathbb{Q}}\right)$ is ramified precisely at p and infinity, for otherwise $\mathcal{H}_p = \emptyset$. Denote $\left(\frac{-d,-p}{\mathbb{Q}}\right)$ simply by B henceforth and let $\{1, i, j, k\}$ be the standard basis of B as in (2.7). We identify K with the subfield $\mathbb{Q}(i)$ of B. Then conjugation by j stabilizes K and sends each $x \in K$ to its complex conjugate $\bar{x}$. Let $\Lambda = \mathcal{O} + j\mathcal{O}$, and S^{opt} be the set of maximal orders in (2.8).

First, we assume that $\mathcal{H}_p \neq \emptyset$ and exhibit a regular action of $\mathrm{Pic}(\mathcal{O})[2]$ on $\mathcal{H}_p$. Since the reduction map $r_{\mathfrak{P}} : \mathcal{E}\ell\ell(\mathcal{O}) \to \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$ is injective by Corollary 2.7, the regular action of $\mathrm{Pic}(\mathcal{O})$ on $\mathcal{E}\ell\ell(\mathcal{O})$ induces a regular action of $\mathrm{Pic}(\mathcal{O})$ on the image $r_{\mathfrak{P}}(\mathcal{E}\ell\ell(\mathcal{O}))$ (or equivalently, on the full set of roots of $\widetilde{H}_{\mathcal{O}}(x)$). We show that this action restricts to a regular $\mathrm{Pic}(\mathcal{O})[2]$-action on $\mathcal{H}_p$.

Proposition 3.1 Let $E_0 \in \mathcal{E}\ell\ell(\mathcal{O})$ be a member satisfying $\mathfrak{j}(\widetilde{E}_0) \in \mathbb{F}_p$. Given $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$, we have $\mathfrak{j}(\widetilde{E_0^{\mathfrak{a}}}) \in \mathbb{F}_p$ if and only if $[\mathfrak{a}]$ is a 2-torsion. In particular, $\mathrm{Pic}(\mathcal{O})[2]$ acts regularly on $\mathcal{H}_p$.

Proof Put $\mathcal{R}_0 := \operatorname{End}(\widetilde{E}_0)$ and $\mathcal{R} := \mathfrak{a}^{-1}\mathcal{R}_0\mathfrak{a}$ so that $\operatorname{End}(\widetilde{E_0^{\mathfrak{a}}}) \simeq \mathcal{R}$ by Corollary 2.2. From Lemma 2.9, it is enough to show that there exists $\alpha \in \mathcal{R}$ with $\alpha^2 = -p$ if and only if $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})[2]$. By Proposition 2.11, we may assume that $\mathcal{R}_0 \in S^{\mathrm{opt}}$, that is, $\mathcal{R}_0$ is a maximal order in B satisfying $\mathcal{R}_0 \supseteq \mathcal{O} + j\mathcal{O}$ and $\mathcal{R}_0 \cap K = \mathcal{O}$. Then

$$\mathcal{R} \cap K = \mathfrak{a}^{-1}(\mathcal{R}_0 \cap K)\mathfrak{a} = \mathcal{O}, \quad \text{and} \quad \mathcal{R} \supseteq \mathfrak{a}^{-1} j \mathfrak{a} = \mathfrak{a}^{-1}\bar{\mathfrak{a}} j. \tag{3.1}$$

First, suppose that $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})[2]$. Then $\mathfrak{a}^{-1}\bar{\mathfrak{a}} = \mathcal{O}a$ for some $a \in K^\times$. Moreover, $N_{K/\mathbb{Q}}(\mathcal{O}a) = N_{K/\mathbb{Q}}(\mathfrak{a}^{-1}\bar{\mathfrak{a}}) = \mathbb{Z}$, so $N_{K/\mathbb{Q}}(a) = 1$. Therefore $\alpha := aj \in \mathcal{R}$ satisfies that $\alpha^2 = a\bar{a}j^2 = -p$.

Conversely, suppose that $\alpha \in \mathcal{R}$ is an element satisfying $\alpha^2 = -p$. From the proof of Proposition 2.11, we must have $\alpha x = \bar{x}\alpha$ for every $x \in \mathcal{O}$. Thus $j^{-1}\alpha$ centralizes $\mathcal{O}$, so there exists $a \in K^\times$ such that $\alpha = ja$. Moreover, $N_{K/\mathbb{Q}}(a) = 1$ since $\alpha^2 = j^2\bar{a}a$. Now we have

$$\mathcal{R} \supset \mathfrak{a}^{-1}\bar{\mathfrak{a}}j \cdot \alpha = \mathfrak{a}^{-1}\bar{\mathfrak{a}}j \cdot ja = -pa\mathfrak{a}^{-1}\bar{\mathfrak{a}}. \tag{3.2}$$

We claim that $\mathcal{R} \supset a\mathfrak{a}^{-1}\bar{\mathfrak{a}}$. It suffices to show that $\mathcal{R}_\ell \supset a\mathfrak{a}_\ell^{-1}\bar{\mathfrak{a}}_\ell$ for every prime $\ell \in \mathbb{N}$, where the subscript $_\ell$ indicates ℓ-adic completion at ℓ. If $\ell \neq p$, then $(-p) \in \mathcal{R}_\ell^\times$, so the containment follows directly from (3.2). If $\ell = p$, then $\mathcal{R}_p$ coincides with the unique maximal order of the division quaternion $\mathbb{Q}_p$-algebra B_p. More concretely, $\mathcal{R}_p = \{z \in B_p \mid \operatorname{nrd}(z) \in \mathbb{Z}_p\}$, where $\operatorname{nrd}(z)$ denotes the reduced norm of $z \in B_p$. On the other hand, for any $x_p \in \mathfrak{a}_p^{-1}$ and $y_p \in \mathfrak{a}_p$, we have $x_p y_p \in \mathcal{O}_p$, and hence $\operatorname{nrd}(ax_p\bar{y}_p) = \operatorname{nrd}(x_p)\operatorname{nrd}(\bar{y}_p) = \operatorname{nrd}(x_p y_p) \in \mathbb{Z}_p$. Since $\mathfrak{a}_p^{-1}\bar{\mathfrak{a}}_p$ is generated by elements of the form $x_p\bar{y}_p$, it follows that $\mathcal{R}_p \supset a\mathfrak{a}_p^{-1}\bar{\mathfrak{a}}_p$. The claim is verified. Now $a\mathfrak{a}^{-1}\bar{\mathfrak{a}} \subseteq \mathcal{R} \cap K = \mathcal{O}$, which implies that $a\bar{\mathfrak{a}} \subseteq \mathfrak{a}$. Comparing discriminants on both sides, we get $\operatorname{disc}(a\bar{\mathfrak{a}}) = N_{K/\mathbb{Q}}(a)^2 \operatorname{disc}(\bar{\mathfrak{a}}) = \operatorname{disc}(\mathfrak{a})$. Therefore, $a\bar{\mathfrak{a}} = \mathfrak{a}$, so $[\mathfrak{a}] \in \operatorname{Pic}(\mathcal{O})[2]$.

Now we drop the assumption that $\mathcal{H}_p \neq \emptyset$ and derive a non-emptiness criterion for $\mathcal{H}_p$. From Proposition 2.11, $\mathcal{H}_p \neq \emptyset$ if and only if $S^{\text{opt}} \neq \emptyset$ (as we have already assumed that $\left(\frac{-d,-p}{\mathbb{Q}}\right) \simeq B_{p,\infty}$). For each prime $\ell \in \mathbb{N}$, let us put

$$S_\ell^{\text{opt}} := \{\mathcal{R}_\ell \subseteq B_\ell \mid \mathcal{R}_\ell \text{ is a maximal order containing } \Lambda_\ell \text{ and } \mathcal{R}_\ell \cap K_\ell = \mathcal{O}_\ell\}.$$

The local-global correspondence of lattices [5, Proposition 4.21] establishes a bijection between S^{opt} and $\prod_\ell S_\ell^{\text{opt}}$, where the product runs over all prime ℓ. Since the reduced discriminant of B is p and the reduced discriminant of Λ is $p\operatorname{disc}(\mathcal{O})$ by [15, Lemmas 2.7 and 2.9], Λ is maximal at every prime ℓ coprime to $\operatorname{disc}(\mathcal{O})$. Moreover, for each such ℓ, the maximal order Λ_ℓ automatically satisfies the condition $\Lambda_\ell \cap K_\ell = \mathcal{O}_\ell$ by its definition $\Lambda_\ell = \mathcal{O}_\ell + j\mathcal{O}_\ell$. Hence for $\ell \nmid \operatorname{disc}(\mathcal{O})$, the set S_ℓ^{opt} has a single element Λ_ℓ, and the bijection above simplifies as

$$S^{\text{opt}} \longleftrightarrow \prod_{\ell \mid \operatorname{disc}(\mathcal{O})} S_\ell^{\text{opt}}. \tag{3.3}$$

Lemma 3.2 Let ℓ be a prime factor of $\operatorname{disc}(\mathcal{O})$. Then $S_\ell^{\text{opt}} \neq \emptyset$ if and only if $-p \in N_{K/\mathbb{Q}}(\mathcal{O}_\ell^\times)$. Moreover, if $S_\ell^{\text{opt}} \neq \emptyset$, then there is a regular action of $H^1(K/\mathbb{Q}, \mathcal{O}_\ell^\times)$ on S_ℓ^{opt}, so any fixed member of S_ℓ^{opt} gives rise to a bijection $S_\ell^{\text{opt}} \simeq H^1(K/\mathbb{Q}, \mathcal{O}_\ell^\times)$.

The Galois cohomological description of S_ℓ^{opt} is nice to know but not used elsewhere in this paper.

Proof By our assumption, $\operatorname{disc}(\mathcal{O})$ is coprime to p, so B splits at the prime ℓ. This allows us to identify B_ℓ with the matrix algebra $M_2(\mathbb{Q}_\ell)$. Let $V_\ell = \mathbb{Q}_\ell^2$ be the unique simple B_ℓ-module. Every maximal order $\mathcal{R}_\ell$ in B_ℓ is of the form $\operatorname{End}_{\mathbb{Z}_\ell}(L_\ell)$ for some $\mathbb{Z}_\ell$-lattice $L_\ell \subseteq V_\ell$, and L_ℓ is uniquely determined by $\mathcal{R}_\ell$ up to $\mathbb{Q}_\ell^\times$-homothety. In other words, $\operatorname{End}_{\mathbb{Z}_\ell}(L_\ell) = \operatorname{End}_{\mathbb{Z}_\ell}(L'_\ell)$ if and only if $L_\ell = cL'_\ell$ for some $c \in \mathbb{Q}_\ell^\times$. If $\mathcal{R}_\ell \in S_\ell^{\text{opt}}$, then the inclusion $\Lambda_\ell \subseteq \mathcal{R}_\ell$ puts a Λ_ℓ-module structure on L_ℓ. Moreover, the Λ_ℓ-lattice L_ℓ is $\mathcal{O}_\ell$-optimal in the sense that $\operatorname{End}_{\mathbb{Z}_\ell}(L_\ell) \cap K_\ell = \mathcal{O}_\ell$. Conversely, if M_ℓ is an $\mathcal{O}_\ell$-optimal Λ_ℓ-lattice in V_ℓ, then $\operatorname{End}_{\mathbb{Z}_\ell}(M_\ell)$ is a member of S_ℓ^{opt}. We have established the following canonical bijection

$$\mathcal{S}_\ell^{\mathrm{opt}} \longleftrightarrow \mathcal{M} := \{\mathcal{O}_\ell\text{-optimal } \Lambda_\ell\text{-lattices } L_\ell \subset V_\ell\}/\mathbb{Q}_\ell^\times. \tag{3.4}$$

Recall that $\Lambda_\ell = \mathcal{O}_\ell + j\mathcal{O}_\ell$, where $j^2 = -p$ and $jx = \bar{x}j$ for any $x \in \mathcal{O}_\ell$. If there exists $a \in \mathcal{O}_\ell^\times$ satisfying $a\bar{a} = -p$, then we can put a Λ_ℓ-module structure on $\mathcal{O}_\ell$ as follows:

$$(x + jy) \cdot z = xz + \bar{y}\bar{z}a, \qquad \forall x, y, z \in \mathcal{O}_\ell.$$

Since $B_\ell = \Lambda_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, this also puts a B_ℓ-module structure on $K_\ell = \mathcal{O}_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Consequently, it identifies K_ℓ with the unique simple B_ℓ-module V_ℓ, and in turn identifies $\mathcal{O}_\ell$ with a Λ_ℓ-lattice L_ℓ in V_ℓ. Necessarily, L_ℓ is $\mathcal{O}_\ell$-optimal since $\mathrm{End}_{\mathbb{Z}_\ell}(L_\ell) \cap K_\ell = \mathrm{End}_{\mathcal{O}_\ell}(L_\ell) = \mathrm{End}_{\mathcal{O}_\ell}(\mathcal{O}_\ell) = \mathcal{O}_\ell$. We have shown that if $-p \in N_{K/\mathbb{Q}}(\mathcal{O}_\ell^\times)$, then $S_\ell^{\mathrm{opt}} \neq \emptyset$.

Conversely, suppose that $S_\ell^{\mathrm{opt}} \neq \emptyset$ and let M_ℓ be an $\mathcal{O}_\ell$-optimal Λ_ℓ-lattice in V_ℓ. The inclusion $\mathcal{O}_\ell \subset \Lambda_\ell$ equips M_ℓ with an $\mathcal{O}_\ell$-module structure satisfying $\mathrm{End}_{\mathcal{O}_\ell}(M_\ell) = \mathcal{O}_\ell$. Being a quadratic $\mathbb{Z}_\ell$-order, $\mathcal{O}_\ell$ is both Gorenstein and semi-local. It follows from [21, Characterization B 4.2] that M_ℓ is a free $\mathcal{O}_\ell$-module of rank one. Pick a basis e so that $M_\ell = \mathcal{O}_\ell e$. Since M_ℓ is at the same time a module over Λ_ℓ, we have $je = ae$ for some $a \in \mathcal{O}_\ell$. Necessarily, $\bar{a}a = -p$ because

$$-pe = j^2e = j(je) = j(ae) = \bar{a}je = \bar{a}ae.$$

This also implies that $a \in \mathcal{O}_\ell^\times$ since $\ell \neq p$. Therefore, $S_\ell^{\mathrm{opt}} \neq \emptyset$ if and only if $-p \in N_{K/\mathbb{Q}}(\mathcal{O}_\ell^\times)$.

Had we picked a different basis e' for M_ℓ, then $e' = ue$ for some $u \in \mathcal{O}_\ell^\times$. It follows that

$$je' = j(ue) = \bar{u}je = \bar{u}ae = u^{-1}\bar{u}ae'.$$

Correspondingly, a is changed to $u^{-1}\bar{u}a$. Therefore, we have defined the following map:

$$\Phi : \mathcal{M} \to \{a \in \mathcal{O}_\ell^\times \mid a\bar{a} = -p\}/\sim, \tag{3.5}$$

where $a \sim a'$ if and only if there exists some $u \in \mathcal{O}_\ell^\times$ such that $a' = a(\bar{u}/u)$. We have already seen that Φ is surjective. Suppose that $\Phi([M_1]) = \Phi([M_2])$ for $[M_r] \in \mathcal{M}$ with $r = 1, 2$. By the above discussion, we can choose suitable $\mathcal{O}_\ell$-base e_r for M_r such that they give rise to the same $a \in \mathcal{O}_\ell^\times$. Then the $\mathcal{O}_\ell$-linear map sending e_1 to e_2 defines a Λ_ℓ-isomorphism between M_1 and M_2. Since $\mathrm{Aut}_{B_\ell}(V_\ell) = \mathbb{Q}_\ell^\times$, it follows that M_1 and M_2 are $\mathbb{Q}_\ell^\times$-homothetic, so Φ is injective as well.

Lastly, if the right hand side of (3.5) is nonempty, then it admits a regular action by $H^1(K/\mathbb{Q}, \mathcal{O}_\ell^\times) = \{b \in \mathcal{O}_\ell^\times \mid \bar{b}b = 1\}/\sim$ via multiplication. The second part of the lemma follows by combining the bijections (3.4) and (3.5) with the above action.

Lemma 3.3 Let ℓ be a prime factor of disc$(\mathcal{O})$. Then $-p \in N_{K/\mathbb{Q}}(\mathcal{O}_\ell^\times)$ if and only if either condition (i) or (ii) below holds for ℓ depending on its parity:

(i) $\ell \neq 2$ and $\left(\frac{-p}{\ell}\right) = 1$;

(ii) $\ell = 2$ and one of the following conditions holds:

(a) $p \equiv 7 \pmod 8$;

(b) $-p + \frac{\mathrm{disc}(\mathcal{O})}{4} \equiv 0$, 1 or $4 \pmod 8$;

(c) $-p + \mathrm{disc}(\mathcal{O}) \equiv 1 \pmod 8$.

Proof For simplicity, put $D := \mathrm{disc}(\mathcal{O})$ and $\delta = \frac{1}{2}\sqrt{D}$. We claim that $\mathcal{O}_\ell = \mathbb{Z}_\ell + \mathbb{Z}_\ell\delta$. It is well known that $\mathcal{O} = \mathbb{Z} + \mathbb{Z}(D + \sqrt{D})/2$. The claim is obviously true if $4|D$. If $4 \nmid D$, then $\ell \neq 2$, so the claim is true in this case as well. Given an element $a + b\delta \in \mathcal{O}_\ell$ with $a, b \in \mathbb{Z}_\ell$, we have $N_{K/\mathbb{Q}}(a + b\delta) = a^2 - b^2 D/4$. Therefore, $-p \in N_{K/\mathbb{Q}}(\mathcal{O}_\ell^\times)$ if and only if the equation

$$x^2 - y^2 \frac{D}{4} = -p \tag{3.6}$$

has a solution in $\mathbb{Z}_\ell^2$.

First, suppose that ℓ is odd. Then equation (3.6) is solvable in $\mathbb{Z}_\ell^2$ if and only if $\left(\frac{-p}{\ell}\right) = 1$. Indeed, suppose $\left(\frac{-p}{\ell}\right) = 1$ so that $-p$ is a square in $\mathbb{F}_\ell$. By Hensel's lemma [23, Lemma 12.2.17], the equation $x^2 = -p$ has a solution $x_0 \in \mathbb{Z}_\ell$. Hence $(x_0, 0)$ is a solution of (3.6) in $\mathbb{Z}_\ell^2$. Conversely, suppose (3.6) has a solution $(x_0, y_0) \in \mathbb{Z}_\ell^2$. Reducing (3.6) modulo ℓ shows that $x_0 \pmod{\ell}$ is a square root of $-p$ in $\mathbb{F}_\ell$, i.e. $\left(\frac{-p}{\ell}\right) = 1$.

For the rest of the proof we assume that $\ell = 2$, which implies that $4|D$. First, suppose that $(x, y) \in \mathbb{Z}_2^2$ is a solution of (3.6). Since x^2, $y^2 \equiv 0$, 1 or $4 \pmod 8$ and at least one of x, y lies in $\mathbb{Z}_2^\times$ because p is odd, we see that the pair (x^2, y^2) takes on five possibilities modulo 8:

$$(x^2, y^2) \equiv (0,1),\ (1,0),\ (1,1),\ (1,4) \text{ and } (4,1) \pmod 8.$$

Each possibility puts the following respective constraint on p and D:

$$-p + \frac{D}{4} \equiv 0 \pmod 8, \qquad -p \equiv 1 \pmod 8, \qquad -p + \frac{D}{4} \equiv 1 \pmod 8,$$
$$-p + D \equiv 1 \pmod 8, \qquad -p + \frac{D}{4} \equiv 4 \pmod 8.$$

We have proved the necessity part of the lemma for the case $\ell = 2$.

Conversely, let us show that the above congruence conditions are also sufficient. From the discussion above, each of these conditions guarantees the existence of a solution $(\tilde{x}, \tilde{y})$ of equation (3.6) in $(\mathbb{Z}/8\mathbb{Z})^2$ such that either $\tilde{x}$ or $\tilde{y}D/4$ lies in $(\mathbb{Z}/8\mathbb{Z})^\times$. Now from a multivariate version of Hensel's lemma [23, Lemma 12.2.8], the pair $(\tilde{x}, \tilde{y})$ lifts to a solution of (3.6) in $\mathbb{Z}_2^2$. The sufficiency is proved.

Therefore, $-p \in N_{K/\mathbb{Q}}(\mathcal{O}_2^\times)$ if and only if one of the following conditions holds:

(a) $p \equiv 7 \pmod 8$;

(b) $-p + \frac{\mathrm{disc}(\mathcal{O})}{4} \equiv 0$, 1 or $4 \pmod 8$;

(c) $-p + \mathrm{disc}(\mathcal{O}) \equiv 1 \pmod 8$.

Proof of Theorem 1.1 If $\mathcal{H}_p \neq \emptyset$, then there is a regular action of $\mathrm{Pic}(\mathcal{O})[2]$ on $\mathcal{H}_p$ by Proposition 3.1. The criterion for the nonemptiness of $\mathcal{H}_p$ follows from combining Proposition 2.11 with equation (3.3) and Lemmas 2.12, 3.2 and 3.3.

References

[1] Amir-Khosravi Z. Serre's tensor construction and moduli of abelian schemes[J]. Manuscripta Math., 2018, 156(3-4): 409-456.

[2] Chai Ching-Li, Conrad Brian, Oort Frans. Complex multiplication and lifting problems[M], Providence, RI: Mathematical Surveys and Monographs, American Mathematical Society, 2014.

[3] Cox D A. Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication[M], New York: Wiley, 1989.

[4] Castryck W, Panny L, Vercauteren F. Rational isogenies from irrational endomorphisms[M]. Lecture Notes in Computer Science vol 12106, Springer, https://doi.org / 10.1007 / 978-3-030-45724-2_18

[5] Curtis C W, Reiner I. Methods of representation theory: with applications to finite groups and orders[M]. New York: Wiley Classics Library, 1990.

[6] Delfs C, Galbraith S D. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$[J]. Designs, Codes and Cryptography, 2016, 78: 425–440

[7] Elkies N D, Ono Ken, Yang Tonghai. Reduction of CM elliptic curves and modular function congruences[J]. International Mathematics Research Notices, 2005, 2(44): 2695-2707.

[8] Gross Benedict H, Zagier Don B. On singular moduli[J]. J. Reine Angew. Math. 1985, 355: 191-220.

[9] Tomoyoshi Ibukiyama. On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings[J]. Nagoya Mathematical Journal,1982, 88: 181-195.

[10] Kaneko M. Supersingular j-invariants as singular moduli $\bmod p$[J], Osaka Journal of Mathematics, 1989, 26(4): 849–855.

[11] Kane Ben. CM liftings of supersingular elliptic curves[J]. J. Théor. Nombres Bordeaux. 2009, 21(3): 635–663.

[12] Lang Serge. Elliptic functions[M]. Graduate Texts in Mathematics with an appendix by J. Tate, New York: Springer-Verlag, 1987.

[13] Li Jianing, Li Songsong, Ouyang Yi. Factorization of Hilbert class polynomials over prime fields[J/OL]. 2021, https://arxiv.org/abs/2108.00168.

[14] Liu S C, Masri Riad, Young Matthew P. Rankin-Selberg L-functions and the reduction of CM elliptic curves[J], Res. Math. Sci., 2015, 2: 22-23.

[15] Li Qun, Xue Jiangwei, Yu Chia Fu. Unit groups of maximal orders in totally definite quaternion algebras over real quadratic fields[J]. Trans. Amer. Math. Soc., 2021, 374(8): 5349–5403.

[16] Milne J S. The fundamental theorem of complex multiplication[J/OL]. 2007, https://arxiv.org/abs/0705.3446.

[17] Onuki Hiroshi. On oriented supersingular elliptic curves[J], Finite Fields Appl. 2021, 69: 18.

[18] Serre J P. A course in arithmetic[M]. Graduate Texts in Mathematics, New York-Heidelberg: Springer-Verlag, 1973.

[19] Shimura Goro. Abelian varieties with complex multiplication and modular functions[M]. Princeton Mathematical Series, Princeton, NJ: Princeton University Press, 1998.

[20] Silverman Joseph H. The arithmetic of elliptic curves[M]. Graduate Texts in Mathematics, Dordrecht: Springer, 2009.

[21] Jensen C U, Thorup Anders. Gorenstein orders[J]. Journal of Pure and Applied Algebra, 2015, 219(3): 551–562.

[22] Vignéras Marie France. Arithmétique des algèbres de quaternions[M]. Lecture Notes in Mathematics, Berlin: Springer,1980.

[23] Voight John. Quaternion algebras[M], Graduate Texts in Mathematics, Cham: Springer,2021.

[24] Waterhouse William C. Abelian varieties over finite fields[J], Ann. Sci. École Norm. Sup. 1969, 04(02): 521–560.

[25] Xiao G J, Luo L X, Deng Y P. Supersingular j-invariants and the class number of $\mathbb{Q}(-p)$[J/OL]. International Journal of Number Theory, https://doi.org/10.1142/S1793042122500555.

希尔伯特类多项式模p的$\mathbb{F}_p$根的个数

陈明洁[1]，薛江维[2]

(1. 美国加利福尼亚大学圣迭戈分校数学系, 加利福尼亚州 92093-0112)

(2. 武汉大学数学与统计学院; 武汉大学数学协同创新中心; 计算科学湖北省重点实验室,
湖北 武汉 430072)

摘 要: 设K是一个虚二次域, $\mathcal{O}$为K中的一个order. 由定义, $\mathcal{O}$的希尔伯特类多项式$H_{\mathcal{O}}(x)$是一个整系数的首一不可约多项式, 它的复根恰为所有具有$\mathcal{O}$-复乘的椭圆曲线的j-不变量. 设$p \in \mathbb{N}$为一个在K中惯性的素数, 且p严格大于$|\operatorname{disc}(\mathcal{O})|$. 若$H_{\mathcal{O}}(x) \pmod p$的$\mathbb{F}_p$根的所组成的集合非空, 我们证明群$\operatorname{Pic}(\mathcal{O})[2]$在该集合上有一个自由且传递的作用; 因此$H_{\mathcal{O}}(x) \pmod p$的$\mathbb{F}_p$根的个数要么等于0, 要么等于$|\operatorname{Pic}(\mathcal{O})[2]|$. 我们还给出了一个关于$\mathbb{F}_p$根存在性的具体判别方法. 类似的结果首先由Xiao 等人在文献[25]中得到, 后又经李等人在文献[13]广泛推广. 本文结果已在李等人的工作中出现, 但方法与之完全不同.

关键词: 希尔伯特类多项式, 超奇异椭圆曲线, 自同态环, 四元数代数, 理想类群

MR(2010)**主题分类号:** 14H52; 11G20; 11R52; 11G15 **中图分类号:** O516.2