Asian J. Math.
Vol. 21, No. 4, pp. 721–774, August 2017

GENUS PERIODS, GENUS POINTS AND CONGRUENT NUMBER PROBLEM[*]

YE TIAN[†], XINYI YUAN[‡], AND SHOU-WU ZHANG[§]

Abstract. In this paper, based on an idea of Tian we establish a new sufficient condition for a positive integer n to be a congruent number in terms of the Legendre symbols for the prime factors of n. Our criterion generalizes previous results of Heegner, Birch–Stephens, Monsky, and Tian, and conjecturally provides a list of positive density of congruent numbers. Our method of proving the criterion is to give formulae for the analytic Tate–Shafarevich number $\mathcal{L}(n)$ in terms of the so-called genus periods and genus points. These formulae are derived from the Waldspurger formula and the generalized Gross–Zagier formula of Yuan–Zhang–Zhang.

Key words. Congruent number, Birch and Swinnerton–Dyer conjecture, Tate–Shafarevich group, Heegner point, Selmer group, Gross–Zagier formula, Waldspurger formula, L–function.

AMS subject classifications. 11G40, 11G05, 11D25.

1. Introduction. A positive integer n is called a *congruent number* if it is the area of a right-angled triangle, all of whose sides have rational lengths. The congruent number problem, the oldest unsolved major problem in number theory, is the question of finding an algorithm for deciding in a finite number of steps whether or not a given integer is a congruent number. In this paper, based on an idea of Tian [26] we will establish a new *sufficient* condition for n to be congruent in terms of the Legendre symbols $\left(\frac{p}{q}\right)$, with p and q running over the prime factors of n.

This type of criterion was first given by Heegner [10] and Birch–Stephens [1] for some n with a single odd prime factor, and by Monsky [18] for some n with two odd prime factors, and finally Tian [26] saw how to extend it to some n with an arbitrary number of prime factors. Our criterion generalizes all of these works, and we believe that it has potential applications to the following *distribution conjecture of congruent numbers*: *all* $n \equiv 5, 6, 7 \pmod 8$ *are congruent and all but density* 0 *of* $n \equiv 1, 2, 3 \pmod 8$ *are not congruent.* Note that in [29], Tunnell gave a *necessary* condition for n to be congruent in terms of the numbers of solutions of some equations $n = Q(x, y, z)$ with positive definite quadratic forms $Q(x, y, z)$ over $\mathbb{Z}$. Tunnell's criterion is also sufficient if the rank part of the BSD conjecture is assumed.

In the following, we would like to describe our main results. Let us first consider the elliptic curve

$$E_n : \quad ny^2 = x^3 - x,$$

where n is assumed to be a *square-free positive* integer throughout this paper. Then it is well known that n is congruent if and only if $E_n(\mathbb{Q})$ has a positive rank. This is equivalent to the vanishing of $L(E_n, 1)$ under the rank part of the Birch-Swinnerton-Dyer (BSD) conjecture

$$\text{rank } E_n(\mathbb{Q}) = \text{ord}_{s=1} L(E_n, s).$$

[*]Received November 28, 2015; accepted for publication February 4, 2016.

[†]Academy of Mathematics and Systems Science, Morningside center of Mathematics, Chinese Academy of Sciences, Beijing 100190, China (ytian@math.ac.cn).

[‡]Department of Mathematics, University of California, Berkeley, CA 94720, USA (yxy@math.berkeley.edu).

[§]Department of Mathematics, Princeton University, Princeton, NJ 08544, USA (shouwu@math.princeton.edu).

By Birch–Stephens [1], the root number

$$\epsilon(E_n) = \begin{cases} 1 & \text{if } n \equiv 1, 2, 3 \pmod 8, \\ -1 & \text{if } n \equiv 5, 6, 7 \pmod 8. \end{cases}$$

It follows that $\mathrm{ord}_{s=1} L(E_n, s)$ is even (resp. odd) if and only if $n \equiv 1, 2, 3 \pmod 8$ (resp. $n \equiv 5, 6, 7 \pmod 8$). The density conjecture of congruent numbers is a consequence of the rank part of the BSD conjecture and the folklore conjecture that $\mathrm{ord}_{s=1} L(E_n, s) \le 1$ for all but a density zero subset of the set of square free positive integers.

By the works of Coates–Wiles [4], Rubin [22], Gross–Zagier [9] and Kolyvagin [17], the rank part of the BSD conjecture holds and the Tate-Shafarevich group is finite whenever $L(E_n, s)$ has a zero of order at most 1 at $s = 1$. Thus we define an invariant $\mathcal{L}(n)$ of E_n as follows:

$$\mathcal{L}(n) := \begin{cases} \left[L(E_n, 1)/(2^{2k(n)-2-a(n)}\Omega_{n,\infty})\right]^{1/2} & \text{if } \mathrm{ord}_{s=1} L(E_n, s) = 0, \\ \left[L'(E_n, 1)/(2^{2k(n)-2-a(n)} \cdot \Omega_{n,\infty} R_n)\right]^{1/2} & \text{if } \mathrm{ord}_{s=1} L(E_n, s) = 1, \\ 0 & \text{if } \mathrm{ord}_{s=1} L(E_n, s) > 1. \end{cases}$$

Here

- $k(n)$ is the number of odd prime factors of n;
- $a(n) = 0$ if n is even, and 1 if n is odd;
- the real period
$$\Omega_{n,\infty} = \frac{2}{\sqrt{n}} \int_1^\infty \frac{dx}{\sqrt{x^3 - x}};$$
- R_n is twice of the Néron–Tate height of a generator of $E_n(\mathbb{Q})/E_n(\mathbb{Q})_{\mathrm{tor}}$ (in the case of rank one).

The definition is made so that, in the case $\mathrm{ord}_{s=1} L(E_n, s) \le 1$, the full BSD conjecture asserts that

$$\#\text{Ш}(E_n) = \mathcal{L}(n)^2. \tag{1.0.1}$$

Moreover, the density conjecture ([5] and [14]), applied to the quadratic twist family E_n, implies that $\mathcal{L}(n)$ *is non-zero for a density one subset of the set of all square free positive integers.*

The number $\mathcal{L}(n)$ is a priori a complex number defined up to a sign. In this paper, we show that $\mathcal{L}(n)$ is an integer (up to a sign), and give a criterion for when it is odd in terms of the parities of the genus class numbers

$$g(d) := \#(2\mathrm{Cl}(\mathbb{Q}(\sqrt{-d})))$$

of positive divisors d of n. It is clear that $g(d)$ is odd if and only if $\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))$ has no element of exact order 4. Thus by Rédei [21], the parity of $g(d)$ can be computed in terms of the Rédei matrix of the Legendre symbols $\left(\frac{p}{q}\right)$ of prime factors p, q of d. The choice of the sign of $\mathcal{L}(n)$ is not an issue in this paper since we are mainly interested in its parity. We divide our results naturally into two cases by the root number $\epsilon(E_n)$.

Theorem 1.1. *Let $n \equiv 1, 2, 3 \pmod 8$ be a positive and square-free integer. Then $\mathcal{L}(n)$ is an integer, and*

$$\mathcal{L}(n) \equiv \sum_{\substack{n=d_0d_1\cdots d_\ell \\ d_i\equiv 1 \pmod 8,\ i>0}} \prod_i g(d_i) \pmod 2.$$

Here all decompositions $n = d_0 \cdots d_\ell$ are non-ordered with $d_i > 1$ for all $i \geq 0$. The right-hand side is considered to be 1 if $n = 1$.

The following theorem is clearly predicted by the BSD conjecture and recently proved by

Theorem 1.2 (Alexander Smith [25], Theorem 4.1 and Corollary 4.2). *For $n \equiv 1, 2, 3 \pmod 8$, the following conditions are equivalent:*

- $\mathrm{rank}_{\mathbb{Z}}(E_n(\mathbb{Q})) = 0$ *and* $\text{Ш}(E_n)[2^\infty] = 0$*;*
- $\displaystyle\sum_{\substack{n=d_0d_1\cdots d_\ell \\ d_i\equiv 1 \pmod 8,\ i>0}} \prod_i g(d_i) \equiv 1 \pmod 2.$

Moreover, the full BSD conjecture holds at a positive proportion of the quadratic twist family E_n.

Combining Theorems 1.1 and 1.2, we obtain the following special case of the conjecture of Birch and Swinnerton-Dyer.

Corollary 1.3. *For every square-free positive integer n congruent to $1, 2$ or 3 modulo 8, we have that $\mathcal{L}(n)$ is odd if and only if $E_n(\mathbb{Q})$ is finite and $\text{Ш}(E_n)[2^\infty] = 0$. Moreover, when these statements holds, $\text{Ш}(E_n)$ finite, and its order is as predicted by the conjecture of Birch and Swinnerton-Dyer.*

Of course, $\text{Ш}(E_n)$ is finite when $\mathcal{L}(n)$ is odd because we then have $L(E_n, 1) \neq 0$, and the statement about the order of $\text{Ш}(E_n)$ then follows from the work of Rubin ([23]) since the corollary proves the 2-primary part of $\text{Ш}(E_n)$ is in accord with the conjecture of Birch and Swinnerton-Dyer. There would be great interest in establishing the analogue of this corollary for the family of quadratic twists of every elliptic curve defined over $\mathbb{Q}$. However, apart from the above result, the analogue of this corollary is only known at present for the family of quadratic twists of the elliptic curve $E = X_0(49)$ ([6] and [3]), where it is proven by the methods of Iwasawa theory, which are very different from those used in this paper.

For $n \equiv 5, 6, 7$, we introduce an integer $\rho(n) \geq 0$ by

$$2^{\rho(n)} = [E_n(\mathbb{Q}) : \varphi_n(A_n(\mathbb{Q})) + E_n[2]],$$

where $\varphi_n : A_n \to E_n$ is a 2-isogeny from $A_n : 2nv^2 = u^3 + u$ to $E_n : ny^2 = x^3 - x$ defined by

$$\varphi_n(u, v) = \left(\frac{1}{2}\left(u + \frac{1}{u}\right), \frac{v}{2u}\left(u - \frac{1}{u}\right)\right).$$

Theorem 1.4. *Let $n \equiv 5, 6, 7 \pmod 8$ be a positive and square-free integer. Then $\mathcal{L}(n)$ is an integer. If $n \equiv 5, 7 \pmod 8$, then $2^{-\rho(n)}\mathcal{L}(n)$ is even only if*

$$\sum_{\substack{n=d_0\cdots d_\ell \\ d_i\equiv 1 \pmod 8,\ i>0}} \prod_i g(d_i) \equiv \sum_{\substack{n=d_0\cdots d_\ell, \\ d_0\equiv 5,6,7 \pmod 8 \\ d_1\equiv 1,2,3 \pmod 8 \\ d_i\equiv 1 \pmod 8,\ i>1}} \prod_i g(d_i) \equiv 0 \pmod 2.$$

If $n \equiv 6 \pmod 8$, then $2^{-\rho(n)}\mathcal{L}(n)$ is even only if

$$\sum_{\substack{n=d_0\cdots d_\ell,\\ d_0\equiv 5,6,7 \pmod 8\\ d_1\equiv 1,2,3 \pmod 8\\ d_i\equiv 1 \pmod 8,\ i>1}} \prod_i g(d_i) \equiv 0 \pmod 2.$$

Here all decompositions $n = d_0 \cdots d_\ell$ are non-ordered with all $d_i > 1$.

Our method of proving these theorems is to give formulae of $\mathcal{L}(n)$ in terms of the so-called genus periods and genus points (cf. Theorems 2.2 and Theorem 3.5). These formulae are derived from the Waldspurger formula in [31] and the generalized Gross–Zagier formula of Yuan–Zhang–Zhang [33] using an induction argument of Tian [26].

Remark 1.5. For each residue class in $\{1, 2, 3, 5, 6, 7 \pmod 8\}$, we believe that our formulae in Theorems 1.1, 1.4 give a positive density of n with $\mathcal{L}(n)$ odd. For $n \equiv 1, 2, 3 \pmod 8$, this is already implied by the BSD formula (1.0.1) modulo 2 and the work of Heath-Brown [11]. Moreover, (1.0.1) modulo 2 can be checked case by case. In fact, in [19], the $\mathbb{F}_2$-rank of $\mathrm{Sel}_2(E_n)/E_n(\mathbb{Q})[2]$ can be also calculated in terms of Legendre symbols for every n.

In the following we give some criteria of congruent numbers and non-congruent numbers extending the work of Tian [26] in terms of a single genus class number.

Corollary 1.6. *Let n be a square-free positive integer such that $\mathbb{Q}(\sqrt{-n})$ has no ideal classes of exact order 4. For any integer r, let A_r, B_r denote the following properties of n:*

$$\begin{aligned} A_r(n): &\quad \#\{p \mid n:\ p \equiv 3 \pmod 4\} \le r;\\ B_r(n): &\quad \#\{p \mid n:\ p \equiv \pm 3 \pmod 8\} \le r. \end{aligned}$$

Then in the following case, n is a non-congruent number:

- $n \equiv 1 \pmod 8$ *with* $A_2(n)$ *or* $B_2(n)$,
- $n \equiv 2 \pmod 8$ *with* $A_0(n)$ *or* $B_2(n)$,
- $n \equiv 3 \pmod 8$ *with* $A_1(n)$ *or* $B_1(n)$.

In the following case, n is a congruent number:

- $n \equiv 5 \pmod 8$ *with* $A_0(n)$ *or* $B_1(n)$,
- $n \equiv 7 \pmod 8$ *with* $A_1(n)$ *or* $B_0(n)$.

Proof. By Rédei [21], $g(d)$ is even in any of the following cases:

- $d = p_1 \cdots p_k \equiv 1 \pmod 8$, $p_i \equiv \pm 1 \pmod 8$, $k > 0$;
- $d = 2p_1 \cdots p_k$, $p_i \equiv \pm 1 \pmod 8$, $k > 0$;
- $d = p_1 \cdots p_k \equiv 1 \pmod 8$, $p_i \equiv 1 \pmod 4$, $k > 0$.

It follows that under any of the conditions of the corollary, the following congruence holds:

$$\sum_{\substack{n=d_0 d_1\cdots d_\ell\\ d_i\equiv 1 \pmod 8,\ i>0}} \prod_i g(d_i) \equiv g(n) \pmod 2.$$

The conclusion follows from Theorem 1.1 and 1.4. □

Acknowledgements. Ye Tian would like to acknowledge the support of the NSFC Grant 11325106, 973 Program 2013CB834202 and the NSFC Grant 11621061. Xinyi Yuan would like to acknowledge the support of the National Science Foundation under the award DMS-1330987. Shou-Wu Zhang would like to acknowledge the support of the National Science Foundation under the awards DMS-0970100 and DMS-1065839.

2. Quadratic periods and genus periods.

The goal of this section is to prove Theorem 1.1. Assume that $n \equiv 1, 2, 3 \pmod 8$ is positive and square-free throughout this section.

2.1. Quadratic periods and genus periods.

Let $K_n = \mathbb{Q}(\sqrt{-n})$ be the quadratic imaginary extension. For any decomposition $n = d_1 \cdot d_2$ with d_2 *positive and odd*, we have an unramified quadratic extension $K_n(\sqrt{d_2^*})$ of K_n where $d_2^* = (-1)^{(d_2-1)/2} d_2$. By the class field theory, the extension gives a quadratic character

$$\chi_{d_1,d_2} : \mathrm{Cl}_n \longrightarrow \{\pm 1\}$$

on the class group Cl_n of K_n. In the degenerate case $d_2 = 1$, we take the convention $\chi_{d_1,d_2} = 1$. Conversely, by Gauss's genus theory, any quadratic character of Cl_n comes from such a decomposition $n = d_1 \cdot d_2$.

The Rankin-Selberg L-series of the elliptic curve $E : y^2 = x^3 - x$ twisted by χ_{d_1,d_2} is given by

$$L(E_{K_n}, \chi_{d_1,d_2}, s) = L(E_{d_1}, s) L(E_{d_2}, s).$$

In the following, we give a formula for $\mathcal{L}(d_1)\mathcal{L}(d_2)$ using the Waldspurger formula. Notice that such formulae concern the quaternion algebra determined by the local root numbers of the L-function $L(E_{K_n}, \chi_{d_1,d_2}, s)$.

Let B be the quaternion algebra over $\mathbb{Q}$ ramified exactly at 2 and ∞. In fact, B is the classical Hamiltonian quaternion algebra (over $\mathbb{Q}$):

$$B = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k, \quad i^2 = j^2 = -1, \ ij = k = -ji.$$

Let O_B be the standard maximal order of B:

$$O_B := O_B' + \mathbb{Z}\zeta, \qquad O_B' := \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k, \qquad \zeta = (-1 + i + j + k)/2.$$

Fix an embedding $\tau : K_n \hookrightarrow B$ such that the image of O_{K_n} lies in O_B. If $n \equiv 1 \pmod 8$, we further specify the embedding by

$$\tau(\sqrt{-n}) = ai + bj + ck$$

where $n = a^2 + b^2 + c^2$ with $a, b, c \in \mathbb{Z}$ and $4|c$. It is a classical result of Legendre that we can find integer solutions a, b, c if n is not of the form $4^e(8m-1)$. The more specific condition $n \equiv 1 \pmod 8$ implies the existence of a solution with $4|c$. See [13, Theorem 5] for example.

By the Jacquet–Langlands correspondence, the newform $f_E \in S_2(\Gamma_0(32))$ corresponding to the elliptic curve $E : y^2 = x^3 - x$ defines an automorphic representation $\pi = \otimes_v \pi_v$ of $B^\times(\mathbb{A})$. Here $\mathbb{A}$ stands for the adéle ring of $\mathbb{Q}$. Let $\widehat{B}$ (resp. $\widehat{\mathbb{Q}}$) denote the finite part of $B(\mathbb{A})$ (resp. $\mathbb{A}$). Note that the central character of π and the infinite part π_∞ are trivial, so $\pi = \otimes_v \pi_v$ is naturally realized as a subspace of $C^\infty(B^\times \backslash \widehat{B}^\times / \widehat{\mathbb{Q}}^\times)$.

Denote by $\pi_\mathbb{Z}$ the $\mathbb{Z}$-submodule of π consisting of elements of π which takes integral values on $B^\times \backslash \widehat{B}^\times / \widehat{\mathbb{Q}}^\times$. Denote $U_n = \widehat{R}_n^\times \cdot K_{n,2}^\times$, an open subgroup of $\widehat{B}^\times$. Here $R_n = O_{K_n} + 4O_B$ is an order of B of conductor 32. Consider the U_n-invariant submodule $\pi_\mathbb{Z}^{U_n}$ of $\pi_\mathbb{Z}$. We will see that $\pi_\mathbb{Z}^{U_n}$ is free of rank 1 over $\mathbb{Z}$, as the special case of $\chi = 1$ in Theorem 2.6. This is an integral example of the multiplicity one theorem of Tunnell [28] and Saito [24] reviewed in Theorem A.1 and Corollary A.2.

Fix a $\mathbb{Z}$-generator f_n of $\pi_\mathbb{Z}^{U_n}$, which is determined up to multiplication by ± 1. Define the *quadratic period* $P(d_1, d_2)$ by

$$P(d_1, d_2) := \sum_{t \in \mathrm{Cl}_n} f_n(t) \chi_{d_1,d_2}(t).$$

Theorem 2.1. *The period $P(d_1, d_2) \neq 0$ only if $d_2 \equiv 1 \pmod 8$. In that case,*

$$P(d_1, d_2) = \pm 2^{k-a} \cdot w_K \cdot \mathcal{L}(d_1)\mathcal{L}(d_2),$$

where $2w_K$ is the number of roots of unity in K, k is the number of odd prime factors of $n = d_1 d_2$, and $a = 1$ if n is odd and $a = 0$ otherwise.

Now we define the *genus period* $Q(n)$ by

$$Q(n) := \sum_{t \in 2\mathrm{Cl}_n} f_n(t).$$

Notice that $P(d_1, d_2)$ and $Q(n)$ are well-defined up to signs.

Theorem 2.2. *The number $\mathcal{L}(n)$ is an integer and satisfies*

$$\mathcal{L}(n) \equiv \sum_{\substack{n = d_0 d_1 \cdots d_\ell \\ d_i \equiv 1 \pmod 8),\ i > 0}} \prod_i Q(d_i) \pmod 2.$$

Here in the sums, all decompositions $n = d_0 \cdots d_\ell$ are non-ordered with $d_i > 1$ for all $i \geq 0$.

Now Theorem 1.1 follows from Theorem 2.2 and the following result.

Proposition 2.3. *One has*

$$f_n\left((\widehat{B}^\times)^2\right) \subset 1 + 2\mathbb{Z}.$$

Therefore,

$$Q(n) \equiv g(n) \pmod 2.$$

Theorems 2.1 and 2.2 and Proposition 2.3 will be proved in section 2.3.

2.2. Primitive test vectors. In this subsection, we give an explicit construction of the test vector f_n, to prepare for the proof of the results in the last subsection.

Resume the above notations related to K_n, B and π. The local components of the automorphic representation $\pi = \otimes_v \pi_v$ of $B^\times(\mathbb{A})$ have the following properties:

- π_∞ is trivial;
- π_p is unramified if $p \neq \infty, 2$, i.e., $\pi^{O_{B,p}^\times}$ is one-dimensional;
- π_2 has a conductor of exponent 4 (cf. [7]), i.e., for a uniformizer λ (for example, $1+i$) of B at 2,

$$\pi_2^{1+\lambda^4 O_{B,2}} \neq 0, \qquad \pi_2^{1+\lambda^3 O_{B,2}} = 0.$$

Let $U = \prod_p U_p$ be the open compact subgroup of $\widehat{O}_B^\times$ with $U_p = O_{B,p}^\times$ if $p \neq 2$, and

$$U_2 = \mathbb{Z}_2^\times (1 + \lambda^4 O_{B,2}) = \mathbb{Z}_2^\times (1 + 4 O_{B,2}).$$

Then $\pi^U \simeq \pi_2^{U_2}$ is stable under the action of $B_2^\times$, since U_2 is normal in $B_2^\times$. By the irreducibility of π_2, we further have $\pi_2^{U_2} = \pi_2$.

By definition, π^U is a subspace of $C^\infty(B^\times \backslash \widehat{B}^\times / \widehat{\mathbb{Q}}^\times U)$, the space of maps from (the finite set) $B^\times \backslash \widehat{B}^\times / \widehat{\mathbb{Q}}^\times U$ to $\mathbb{C}$. The following is a more detailed description.

Theorem 2.4.

(1) *The space π^U is a 6-dimensional irreducible representation of $B_2^\times$, with an orthogonal basis*

$$f_\delta \in C^\infty(B^\times \backslash \widehat{B}^\times / \widehat{\mathbb{Q}}^\times U), \qquad \delta \in \left\{ \frac{\pm i \pm j}{2}, \frac{\pm j \pm k}{2}, \frac{\pm k \pm i}{2} \right\} \Big/ \{\pm 1\}.$$

Here for each δ, the function f_δ is determined by its restriction to $1 + 2O_{B,2}$ and

$$f_\delta(1+2x) = (-1)^{\mathrm{Tr}(\delta x)}, \qquad \forall x \in O_{B,2}.$$

(2) *The representation π^U of $B_2^\times$ has an integral structure $\pi_{\mathbb{Z}}^U$ generated by*

$$f_{i \pm j} := \frac{1}{2}(f_{\frac{i+j}{2}} \pm f_{\frac{i-j}{2}}), \quad f_{j \pm k} := \frac{1}{2}(f_{\frac{j+k}{2}} \pm f_{\frac{j-k}{2}}), \quad f_{k \pm i} := \frac{1}{2}(f_{\frac{k+i}{2}} \pm f_{\frac{k-i}{2}}).$$

Moreover, this $\mathbb{Z}$-basis is orthonormal with respect to the Tamagawa measure on $B^\times \backslash B^\times(\mathbb{A}) / \mathbb{A}^\times$.

(3) *Let χ_0 be the character of $B^\times(\mathbb{A})$ associated to the quadratic extension $\mathbb{Q}(i)$, i.e. the composition*

$$B^\times(\mathbb{A}) \xrightarrow{\det} \mathbb{A}^\times \simeq \mathbb{Q}^\times \times (\widehat{\mathbb{Z}}^\times \times \mathbb{R}_+^\times) \longrightarrow \widehat{\mathbb{Z}}^\times \longrightarrow (\mathbb{Z}/4\mathbb{Z})^\times \simeq \{\pm 1\}.$$

Then $\pi \simeq \pi \otimes \chi_0$ and

$$\chi_0 f_{\frac{i+j}{2}} = f_{\frac{i-j}{2}}, \qquad \chi_0 f_{\frac{j+k}{2}} = f_{\frac{j-k}{2}}, \qquad \chi_0 f_{\frac{k+i}{2}} = f_{\frac{k-i}{2}}.$$

To deduce the theorem, we first need the following precise description of $B^\times \backslash \widehat{B}^\times / \widehat{\mathbb{Q}}^\times U$.

Lemma 2.5. *The following natural maps are bijective:*

$$O_{B,2}/(\mathbb{Z}_2 + 2O_{B,2}) \xrightarrow{\sim} (1 + 2O_{B,2})/\mathbb{Z}_2^\times(1 + 4O_{B,2}) \xrightarrow{\sim} B^\times \backslash \widehat{B}^\times / \widehat{\mathbb{Q}}^\times U,$$

where the first map is defined by $x \mapsto 1+2x$, and the second one is given by the natural inclusion $B_2^\times \subset \widehat{B}^\times$.

Moreover, under the composition

$$B^\times\backslash B^\times(\mathbb{A})/\widehat{\mathbb{Q}}^\times \longrightarrow B^\times\backslash\widehat{B}^\times/\widehat{\mathbb{Q}}^\times U \xrightarrow{\sim} O_{B,2}/(\mathbb{Z}_2+2O_{B,2}),$$

the Tamagawa measure on $B^\times\backslash B^\times(\mathbb{A})/\mathbb{A}^\times$ transfers to the Haar measure of (the finite abelian group) $O_{B,2}/(\mathbb{Z}_2+2O_{B,2})$ of total volume 2.

Proof. We first prove the bijectivity. The first map is clearly a group isomorphism. For the second map, we use the class number one property of B, i.e.,

$$\widehat{B}^\times = B^\times\cdot\widehat{O}_B^\times = B^\times\cdot B_2^\times\cdot U^{(2)}.$$

Here $U^{(2)}$ denotes the subgroup of U with 2-component 1. It follows that

$$B^\times\backslash\widehat{B}^\times/\widehat{\mathbb{Q}}^\times U \simeq H\backslash B_2^\times/\mathbb{Q}_2^\times U_2, \quad H = B^\times\cap(U^{(2)}\cdot B_2^\times).$$

It is easy to see that H is a semi-product of $\lambda^{\mathbb{Z}}$, where $\lambda\in O_B$ is an element with reduced norm 2, and the subgroup

$$O_B^\times = \left\{\pm1, \quad \pm i, \quad \pm j, \quad \pm k, \quad \frac{\pm1\pm i\pm j\pm k}{2}\right\}.$$

The group $O_B^\times$ is a semi-product of μ_3 generated by $\zeta=(-1+i+j+k)/2$ and

$$(O_B')^\times = \{\pm1, \quad \pm i, \quad \pm j, \quad \pm k\}.$$

Consider the filtration of $B_2^\times$ given by

$$B_2^\times \supset O_{B,2}^\times \supset 1+\lambda O_{B,2}^\times \supset 1+2O_{B,2},$$

and its induced filtration

$$H\supset O_B^\times\supset(O_B')^\times\supset\mu_2.$$

It is straight forward to check that these two exact sequences have isomorphic subquotients. It follows that the map $H\to B_2^\times$ induces an exact sequence

$$1\longrightarrow\mu_2\longrightarrow H\longrightarrow B_2^\times/(1+2O_{B,2})\longrightarrow 1.$$

In other words, the $B_2^\times$ is generated by H and the normal subgroup $1+2O_{B,2}$ with intersection $H\cap(1+2O_{B,2})=\mu_2$. Thus

$$H\backslash B_2^\times/\mathbb{Q}_2^\times U_2 \xleftarrow{\sim} \mu_2\backslash(1+2O_{B,2}/1+4O_{B,2}) \xleftarrow{\sim} (1+2O_{B,2})/\mathbb{Z}_2^\times(1+4O_{B,2}).$$

The other two relations can be verified similarly.

Now we treat the measure. Note that the Tamagawa measure gives $B^\times\backslash B^\times(\mathbb{A})/\mathbb{A}^\times$ total volume 2. Then the induced measure on $O_{B,2}/(\mathbb{Z}_2+2O_{B,2})$ also has total volume 2. It suffices to check that the induced measure is uniform. Equivalently, we need to show that $\mathrm{vol}(B^\times\backslash B^\times g\widehat{\mathbb{Q}}^\times U)$ is constant in $g\in\widehat{B}^\times$. By the first part of the lemma, we can always take a representative $g\in 1+2O_{B,2}$ for the double coset $B^\times g\widehat{\mathbb{Q}}^\times U$. The key is that $g_p=1$ for $p\neq 2$. It follows that

$$B^\times\backslash B^\times g\widehat{\mathbb{Q}}^\times U = B^\times\backslash B^\times\widehat{\mathbb{Q}}^\times Ug,$$

whose volume is independent of g since the measure is invariant under the right translation. □

In the lemma, the right multiplication action of $B_2^\times = H \cdot (1 + 2O_{B,2})$ on $\widehat{B}^\times$ induces its action on $O_{B,2}/(\mathbb{Z}_2 + 2O_{B,2})$ given by right conjugation of H and translation of x, for elements $1 + 2x \in 1 + 2O_{B,2}$.

Consider the space $\mathcal{A}_0 \subseteq C^\infty(B^\times \backslash \widehat{B}^\times / \widehat{\mathbb{Q}}^\times)$ of forms perpendicular to forms $\chi \circ \det$ where χ runs over all characters of $\mathbb{Q}^\times \backslash \widehat{\mathbb{Q}}^\times$, then $\pi \subset \mathcal{A}_0$. Let $\mathcal{A}_0^U$ be the subspace of $\mathcal{A}_0$ of forms invariant under U, then $\pi^U \subset \mathcal{A}_0^U$.

The restriction map

$$\mathcal{A}_0^U \longrightarrow \mathbb{C}[O_{B,2}/(\mathbb{Z}_2 + 2O_{B,2})], \qquad f \longmapsto (\phi_f : x \mapsto f(1 + 2x))$$

defines an isomorphism between $\mathcal{A}_0^U$ and the space $\mathcal{A}_1$ of functions ϕ on $O_{B,2}/(\mathbb{Z}_2 + 2O_{B,2})$ perpendicular to the characters 1 and $(-1)^{\mathrm{Tr}}$ on $O_{B,2}/(\mathbb{Z}_2 + 2O_{B,2})$. Here the trace map

$$\mathrm{Tr} : O_{B,2}/(\mathbb{Z}_2 + 2O_{B,2}) \longrightarrow \mathbb{Z}_2/2\mathbb{Z}_2$$

is induced form the reduced trace. The vector space $\mathcal{A}_1$ is decomposed into the direct sum

$$\mathcal{A}_1 = \sum_{\psi \in \Psi} \mathbb{C}\psi,$$

where

$$\Psi = \left\{\psi \in \mathrm{Hom}(O_B/(2O_B + \mathbb{Z}), \mu_2), \quad \psi \neq 1, (-1)^{\mathrm{Tr}}\right\}$$

is a set of quadratic characters ψ of $O_{B,2}/(\mathbb{Z}_2 + 2O_{B,2})$.

We have an explicit description of forms in $\mathcal{A}_0^U$ corresponding to Ψ. Let $\wp = \lambda O_{B,2}$ be the maximal ideal of $O_{B,2}$. Then the trace map defines a perfect pairing

$$O_{B,2} \otimes \wp^{-1} \longrightarrow \mathbb{Z}_p, \qquad (x, y) \longrightarrow \mathrm{Tr}(xy).$$

It induces a perfect pairing

$$(O_{B,2}/2O_{B,2}) \otimes (\wp^{-1}/2\wp^{-1}) \longrightarrow \mu_2, \qquad (x, y) \mapsto (-1)^{\mathrm{Tr}(xy)}.$$

It is easy to see that Ψ corresponds to the subset $\bar{\Delta}$ of elements $\bar{\delta} \in \wp^{-1}/2\wp^{-1}$ with the following properties:

$$\mathrm{Tr}(\delta) = 0 \,(\mathrm{mod}\, 2), \qquad \delta \neq 0, 1 \,(\mathrm{mod}\, 2).$$

Note that the set

$$\Delta = \left\{\frac{\pm i \pm j}{2}, \frac{\pm j \pm k}{2}, \frac{\pm k \pm i}{2}\right\}$$

in Theorem 2.4 is contained in $\wp^{-1}$. Thus we can identify $\bar{\Delta} = \Delta/\{\pm 1\}$. For each $\delta \in \Delta/\{\pm 1\}$, the corresponding form f_δ is given by

$$f_\delta(g) = (-1)^{\mathrm{Tr}(\delta x)},$$

for any $g = bh(1+2x)u \in \widehat{B}^\times$ with $b \in B^\times$, $h \in H$, $x \in O_{B,2}$, and $u \in \widehat{\mathbb{Q}}^\times U$. Hence, the space $\mathcal{A}_0^U$ is 6-dimensional with the explicit decomposition

$$\mathcal{A}_0^U = \sum_{\delta \in \Delta/\{\pm 1\}} \mathbb{C} f_\delta$$

into characters of $(1+2O_{B,2})/(1+4O_{B,2})$.

Proof of Theorem 2.4. For (1), it suffices to prove that $\mathcal{A}_0^U$ is irreducible as a representation of $G := B_2^\times/(1+4O_{B,2})$. Note that G contains a normal and commutative finite subgroup $C = (1+2O_{B,2})/(1+4O_{B,2})$. Thus any invariant subspace V of $\mathcal{A}_0^U$ is a direct sum

$$V = \oplus_{\chi \in X} V_\chi$$

over some multiset X of characters of C. The multiset X is stable under the conjugation of G. We have seen that V_χ are all one-dimensional, and X is included into Ψ, the set of characters induced by elements in Δ. Thus we need only prove that G acts transitively on Δ by conjugations. In fact, Δ is a principal homogenous space of $O_B^\times/\mu_2$ under conjugation.

Now we treat (2). Note that for any $h \in H$, $x \in O_{B,2}$, and $\delta \in \Delta$, we have that $h\delta h^{-1} \in \Delta$ and

$$\pi(h(1+2x))f_\delta = \psi_\delta(x) f_{h\delta h^{-1}} = \pm f_{h\delta h^{-1}},$$

where $\psi_\delta \in \Psi$ denotes the character $x \mapsto (-1)^{\mathrm{Tr}(\delta x)}$ on $O_{B,2}/(\mathbb{Z}_2 + 2O_{B,2})$. Therefore, the action of $B_2^\times$ on $f_{i\pm j}$ is given by

$$\pi(h)f_{i\pm j} = f_{hih^{-1} \pm hjh^{-1}}, \qquad \pi(1+2x)f_{i\pm j} \in \{\pm f_{i+j}, \pm f_{i-j}\}.$$

Similar results hold for $f_{j\pm k}$ and $f_{k\pm i}$. Thus $\pi_{\mathbb{Z}}^U$ is an integral structure on π^U. The orthonormality of the basis is a simple consequence of the previous result on the measures.

For (3), it is clear that χ_0 is invariant under the left action of $B^\times \cdot H$ and the right action of U and its restriction on $1+2O_{B,2}$ is given by $\chi_0(1+2x) = (-1)^{\mathrm{Tr} x}$ for any $x \in O_{B,2}$. Thus for any $x \in O_{B,2}$,

$$\chi_0 f_{\frac{i+j}{2}}(1+2x) = (-1)^{\mathrm{Tr}(x + \frac{i+j}{2}x)} = (-1)^{\mathrm{Tr}(x\frac{i-j}{2})}(-1)^{\mathrm{Tr}((1+j)x)} = f_{\frac{i-j}{2}}(1+2x).$$

□

THEOREM 2.6. *Let K be an imaginary quadratic field and χ a quadratic character of $\widehat{K}^\times/K^\times\widehat{O}_K^\times$ such that $L(E_K,\chi,s)$ has root number $+1$ (so that 2 cannot split in K). Let ϖ be a uniformizer of K_2 and χ_2 the 2-component of χ. Fix a $\mathbb{Q}$-embedding $\tau : K \hookrightarrow B$ such that O_K is contained in O_B. Then the vector space*

$$\pi^{U,\chi_2} := \{f \in \pi^U,\ \pi(t)f = \chi_2(t)f,\ \forall t \in K_2^\times\}$$

is one-dimensional. All the possible cases of $(K_2, \chi_2(\varpi))$ are listed below:

$$(\mathbb{Q}_2(\sqrt{-3}), 1), \quad (\mathbb{Q}_2(\sqrt{-1}), \pm 1), \quad (\mathbb{Q}_2(\sqrt{-2m}), (-1)^{\frac{m-1}{2}}),\ m \equiv 1,3,5,7 \pmod 8.$$

Let $g \in B_2^\times$ be such that $\tau_2' := g^{-1}\tau_2 g$ is given by

$$\begin{aligned} &(-1+\sqrt{-3})/2 \longmapsto \zeta, \quad \sqrt{-1} \longmapsto k, \quad &&\sqrt{-2} \longmapsto i+j,\\ &\sqrt{-10} \longmapsto i-3j, \quad \sqrt{-6} \longmapsto i+j+2k, \quad &&\sqrt{-14} \longmapsto -3i+j-2k, \end{aligned}$$

respectively in the above cases. Then the vector $f = \pi(g) f_0$ lies in π^{U,χ_2}, where

$$f_0 = \begin{cases} f_{\frac{i-j}{2}} + f_{\frac{j-k}{2}} + f_{\frac{k-i}{2}}, & \text{if } K_2 = \mathbb{Q}_2(\sqrt{-3}),\\ f_{i \pm j} = \frac{1}{2}\left(f_{\frac{i+j}{2}} \pm f_{\frac{i-j}{2}}\right), & \text{if } (K_2, \chi_2(\varpi)) = (\mathbb{Q}_2(\sqrt{-1}), \pm 1),\\ f_{\frac{i+j}{2}}, & \text{if } K_2 = \mathbb{Q}_2(\sqrt{-2m}) \text{ with } m \text{ odd.} \end{cases}$$

Moreover, $\pi_{\mathbb{Z}}^{U,\chi_2} := \pi_{\mathbb{Z}}^U \cap \pi^{U,\chi_2} = \mathbb{Z} f$.

Definition 2.7. The automorphic forms f and $-f$ described in the theorem are called *primitive test vectors* for (π, χ).

The theorem can be interpreted by the multiplicity one theorem of Tunnell [28] and Saito [24] reviewed in Theorem A.1 and Corollary A.2. In fact, the space

$$\pi^{\widehat{O}_B^{2,\times}, \chi_2} := \{ f \in \pi^{\widehat{O}_B^{2,\times}}, \ \pi(t) f = \chi_2(t) f, \ \forall t \in K_2^\times \}$$

is at most one-dimensional by the multiplicity one theorem. The theorem confirms that it is one-dimensional and constructs an explicit generator of the integral structure.

Proof of Theorem 2.6. It suffices to show that f_0 is χ_2-invariant under the embedding $\tau_2' : K \hookrightarrow B$.

First consider the case $K_2 = \mathbb{Q}_2(\sqrt{-3})$, where

$$K_2^\times / \mathbb{Q}_2^\times (1 + 4O_2) = O_2^\times / \mathbb{Z}_2^\times (1 + 4O_2)$$

is cyclic of order 6 and generated by ζ and $1 + 2\zeta$. Note that

$$\zeta^{-1} i \zeta = j, \quad \zeta^{-1} j \zeta = k, \quad \zeta^{-1} k \zeta = i.$$

Thus the subspace of π^U of forms fixed by $\zeta \in H$ is 2-dimensional with basis

$$f_{\frac{i-j}{2}} + f_{\frac{j-k}{2}} + f_{\frac{k-i}{2}}, \quad f_{\frac{i+j}{2}} + f_{\frac{j+k}{2}} + f_{\frac{k+i}{2}}.$$

Moreover, note that $\psi_\delta(\zeta) = 1$ for $\delta = \frac{i-j}{2}, \frac{j-k}{2}, \frac{k-i}{2}$ and $\psi_\delta(\zeta) = -1$ otherwise. Thus π^{U,χ_2} is one-dimensional with basis $f_{\frac{i-j}{2}} + f_{\frac{j-k}{2}} + f_{\frac{k-i}{2}}$.

In the case $K_2 = \mathbb{Q}(\sqrt{-1})$, let $\varpi = k - 1$, we have that

$$K_2^\times / \mathbb{Q}_2^\times (1 + 4O_2) = \varpi^{\mathbb{Z}/4\mathbb{Z}} \times \langle 1 + \varpi, 1 + 2\varpi \rangle.$$

Note that $1 + 2\varpi = 2k - 1$, and $\psi_\delta(k) = 1$ if $\delta = \frac{i \pm j}{2}$ and $\psi_\delta(k) = -1$ otherwise. Thus the subspace of π^U of forms fixed by $1 + 2\varpi$ is 2-dimensional with basis

$$f_{i+j}, \quad f_{i-j},$$

where $1 + \varpi = k$ acts trivially since $k^{-1} i k = -i, k^{-1} j k = -j$. Finally, since $\varpi = k - 1 \in H$ and

$$\varpi^{-1} i \varpi = j, \quad \varpi^{-1} j \varpi = -i, \varpi^{-1} k \varpi = k,$$

we have that π^{U,χ_2} is one-dimensional with basis $f_{i\pm j}$ for $\chi_2(\varpi)=\pm 1$.

For the case $K_2=\mathbb{Q}_2(\sqrt{-2n})$ with $n=1,3,5,7$, let $\varpi=\sqrt{-2n}$, we have that $K_2^\times/\mathbb{Q}_2^\times(1+4O_2)$ is generated by the order 2 element ϖ and order 4 element $1+\varpi$. The embedding τ_2' maps $1+\varpi$ to $k(1+2(\zeta+i)) \bmod \mathbb{Z}_2^\times(1+4O_{B,2})$. Note that $kik^{-1}=-i, kjk^{-1}=-j$ and

$$\psi_\delta(\zeta+i)=\begin{cases}1, & \text{if } \delta=\frac{i+j}{2},\frac{i+k}{2},\frac{j-k}{2},\\ -1, & \text{otherwise.}\end{cases}$$

It follows that the subspace of π^U fixed by $\tau_2'(1+\varpi)$ is one-dimensional with basis $f_{\frac{i+j}{2}}$. We have the following decompositions of $\tau_2'(\varpi)\in B_2^\times=H\cdot(1+2O_{B,2}) \bmod \mathbb{Z}_2^\times(1+4O_{B,2})$:

$$\begin{aligned} &i+j\in H, && i-3j\equiv(i+j)(1+2k),\\ &i+j+2k\equiv(j-i)(1+2(\zeta-k)), && -3i+j-2k=(i-j)(1+2(\zeta-k)). \end{aligned}$$

Note that $\psi_{\frac{i+j}{2}}(k)=1$ and $\psi_{\frac{i+j}{2}}(\zeta)=-1$, we know that $f_{\frac{i+j}{2}}$ is χ_2-invariant. □

2.3. Proofs of Theorems 2.1, 2.2 and Proposition 2.3 . Resume the notations in §2.1. Especially, f_n is a basis of $\pi_{\mathbb{Z}}^{U_n}$ with

$$U_n=\widehat{R}_n^\times\cdot K_{n,2}^\times,\quad R_n=O_{K_n}+4O_B.$$

We first connect it to the primitive test vectors in §2.2.

Recall that in §2.2, we have introduced

$$U=\widehat{O}_B^{2,\times}\cdot U_2,\quad U_2=\mathbb{Z}_2^\times(1+4O_{B,2}).$$

In Theorem 2.6 and Definition 2.7, we have introduced the primitive test vectors for (π,χ). For the connection, it is easy to verify $U_n=U\cdot K_{n,2}^\times$. Hence, f_n is a primitive test vector for (π,χ) if and only if $\chi_2=1$.

Proof of Theorem 2.1. Write $K=K_n$ for simplicity. The goal is to treat

$$P(d_1,d_2)=\sum_{t\in \mathrm{Cl}_n} f_n(t)\chi_{d_1,d_2}(t).$$

The tool is the Waldspurger formula.

By $\mathrm{Cl}_n=K^\times\backslash\widehat{K}^\times/\widehat{O}_K^\times$, the summation is essentially an integration on $K^\times\backslash\widehat{K}^\times$. Since f_n is invariant under the action of $K_2^\times$, the integration is nonzero only if χ_{d_1,d_2} is trivial on $K_2^\times$. In other words, $K_2(\sqrt{d_2^*})$ splits into two copies of $K_2=\mathbb{Q}_2(\sqrt{-n})$. This is equivalent to $d_2^*\equiv 1 \pmod 8$. Then $d_2\equiv\pm1 \pmod 8$. We will exclude the case $d_2\equiv -1 \pmod 8$ later.

Assume $d_2^*\equiv 1 \pmod 8$. Then χ_{d_1,d_2} is trivial on $K_2^\times$, and f_n is a primitive test vector for (π,χ_{d_1,d_2}) as described in Theorem 2.6. In particular,

$$(f_n,f_n)_{\mathrm{Pet}}=\begin{cases}6, & \text{if } K_2=\mathbb{Q}_2(\sqrt{-3}),\\ 1, & \text{if } K_2=\mathbb{Q}_2(\sqrt{-1}),\\ 2, & \text{if } K_2=\mathbb{Q}_2(\sqrt{-2m}) \text{ with } m=1,3,5,7.\end{cases}$$

Apply the explicit Waldspurger formula in Theorem A.4. We have

$$|P(d_1,d_2)|^2=\frac{w_K^2}{2^5 3^b\pi^3}\cdot\frac{(f_n,f_n)_{\mathrm{Pet}}}{(f',f')_{\mathrm{Pet}}}\cdot L(E_{d_1},1)L(E_{d_2},1),$$

where $b = 1$ if 2 is inert in K and $b = 0$ otherwise, and f' is the normalized new form in the automorphic representation of $\mathrm{GL}_2(\mathbb{A})$ associated to E.

We claim that

$$(f', f')_{\mathrm{Pet}} = \Omega_{d_1,\infty}\Omega_{d_2,\infty} \cdot \frac{|D|^{1/2}}{2^8\pi^3 e},$$

where D is the discriminant of K and $e = 1$ if $2 \nmid D$ and $e = 2$ otherwise. Let $\phi = \sum_{n=1}^{\infty} a_n q^n$ be the corresponding newform of weight 2. Note that

$$(\phi, \phi)_{\Gamma_0(32)} = \iint_{\Gamma_0(32)\backslash\mathcal{H}} |\phi(z)|^2 dxdy$$

and

$$(f', f')_{\mathrm{Pet}} = \int_{\mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A})/\mathbb{Q}^\times} |f'(g)|^2 dg$$

are related by

$$\frac{(\phi, \phi)_{\Gamma_0(32)}}{\mathrm{vol}(X_0(32))} = \frac{(f', f')_{\mathrm{Pet}}}{2}, \qquad \text{where } \mathrm{vol}(X_0(32)) = 16\pi.$$

Let $\varphi : X_0(32) \to E$ be a modular parametrization of degree 2, and ω the Néron differential on E, and $\Omega = \int_{E(\mathbb{R})} \omega$. Note that

$$\varphi^*\omega = 4\pi i\phi(z)dz, \quad 2^{-1}\Omega^2 = \iint_{E(\mathbb{C})} |\omega \wedge \overline{\omega}|,$$

and thus

$$\Omega^2 = 32\pi^2(\phi, \phi)_{\Gamma_0(32)}.$$

By definition,

$$\Omega_{d_1,\infty}\Omega_{d_2,\infty} = \Omega^2/\sqrt{d_1 d_2} = 2^{e-1}\Omega^2/\sqrt{|D|}.$$

Put all these together, we have the formula for $(f'f')_{\mathrm{Pet}}$.

Hence, we have

$$|P(d_1, d_2)|^2 = 2^{4+c} w_K^2 \frac{L(E_{d_1}, 1)}{\Omega_{d_1,\infty}} \cdot \frac{L(E_{d_2}, 1)}{\Omega_{d_2,\infty}},$$

where $c = 0$ if $8 \nmid D$ and $c = 1$ otherwise. It gives the formula of the theorem.

It remains to prove that $d_2 \equiv -1 \pmod 8$ implies $P(d_1, d_2) = 0$. This is a direct consequence from the formula we just proved, since $L(E_{d_1}, 1) = 0$ by considering the root number in this case.

Proof of Theorem 2.2. Let $h_2(n) = \dim_{\mathbb{F}_2} \mathrm{Cl}_n/2\mathrm{Cl}_n$. By Gauss's genus theory, $h_2(n) + 1$ is exactly equal to the number of prime factors of the discriminant of K_n, and any character of $\mathrm{Cl}_n/2\mathrm{Cl}_n$ is of the form χ_{d_1,d_2} for some decomposition $d = d_1 d_2$ with d_2 positive and odd. Moreover, a repetition $\chi_{d_1',d_2'} = \chi_{d_1,d_2}$ occurs only if $(d_1', d_2') = (d_2, d_1)$ and $n \equiv 3 \pmod 8$.

Hence, we have the character formula

$$\sum_{n=d_1d_2}{}' \chi_{d_1,d_2}(t) = 2^{h_2(n)}\delta_{2\mathrm{Cl}(K_n)}(t), \qquad t \in \mathrm{Cl}_n,$$

where the sum is over ordered (resp. non-ordered) decompositions $d = d_1d_2$ if $n \equiv 1 \pmod 8$ (resp. $n \equiv 3 \pmod 8$), and requires d_2 to be odd if $n \equiv 2 \pmod 8$. As a result, we have

$$\sum_{n=d_1d_2}{}' P(d_1, d_2) = 2^{h_2(n)}Q(n). \tag{2.3.1}$$

The summation follows the same rule as above.

The following lemma shows the symmetry in the case $n \equiv 1 \pmod 8$.

Lemma 2.8. *Assume $n \equiv 1 \pmod 8$. Then for any decomposition $d = d_1d_2$ with $d_1, d_2 > 0$,*

$$P(d_1, d_2) = P(d_2, d_1).$$

Proof. Let χ_0 be the character on $\widehat{B}^\times$ corresponding to the extension $\mathbb{Q}(i)$ over $\mathbb{Q}$, defined in Theorem 2.4. The two quadratic characters are related by

$$\chi_{d_1,d_2} = \chi_{d_2,d_1} \cdot \chi_0.$$

In fact, for any $t \in \widehat{K}^\times$, we have

$$\chi_{d_1,d_2}(t)\chi_{d_2,d_1}(t) = \frac{\sigma_t(\sqrt{d_1})}{\sqrt{d_1}}\frac{\sigma_t(\sqrt{d_2})}{\sqrt{d_2}} = \frac{\sigma_t(i)}{i} = \chi_0(t).$$

In the notation of Theorem 2.6, the primitive test vector is given by $f_n = \pi(g)f_0$ (up to $\{\pm 1\}$) with $g \in B_2^\times$ and

$$f_0 = \frac{1}{2}(f_{\frac{i+j}{2}} + f_{\frac{i-j}{2}}) = f_{\frac{i+j}{2}} \cdot (\frac{1+\chi_0}{2}).$$

We claim that $\chi_0(g) = 1$ by our special choice of $\tau : K_n \hookrightarrow B$ at the beginning.

Assuming $\chi_0(g) = 1$, then

$$\begin{aligned} P(d_2, d_1) &= \sum_t f_{\frac{i+j}{2}}(tg)\frac{1+\chi_0(t)}{2}\chi_{d_2,d_1}(t) \\ &= \sum_t f_{\frac{i+j}{2}}(tg)\frac{1+\chi_0(t)}{2}\chi_0(t)\chi_{d_1,d_2}(t) \\ &= \sum_t f_{\frac{i+j}{2}}(tg)\frac{1+\chi_0(t)}{2}\chi_{d_1,d_2}(t) \\ &= P(d_1, d_2). \end{aligned}$$

It remains to check $\chi_0(g) = 1$. Recall that $g \in B_2^\times$ is an element such that $\tau_2' = g^{-1}\tau_2 g : K_{n,2} \hookrightarrow B_2$ gives $\tau_2'(\sqrt{-1}) = k$. Recall that the embedding $\tau : K_n \hookrightarrow B$ is defined by

$$\tau(\sqrt{-n}) = ai + bj + ck$$

where $n = a^2 + b^2 + c^2$ with $a, b, c \in \mathbb{Z}$ and $4|c$. Thus the equation for g is just

$$g^{-1} \cdot \frac{1}{\sqrt{n}}(ai + bj + ck) \cdot g = k.$$

Here $\sqrt{n}$ denotes a square root of n in K_2. Explicit computation gives a solution

$$g_0 = ai + bj + (c + \sqrt{n})k.$$

For this solution, we have

$$\det(g_0) = a^2 + b^2 + (c + \sqrt{n})^2 = 2(n + c\sqrt{n}).$$

Note that $n + c\sqrt{n} \equiv 1 \pmod 4$ by the condition $4|c$, and thus $\chi_0(g_0) = 1$. It is easy to see that any other solution is of the form $g = g_0(u + vk)$ for $u, v \in \mathbb{Q}_2$. Then we have $\chi_0(u + vk) = 1$ and thus $\chi_0(g) = 1$. □

LEMMA 2.9. *One has*

$$\sum_{n=d_1d_2} \epsilon(d_1, d_2)\mathcal{L}(d_1)\mathcal{L}(d_2) = Q(n),$$

where $\epsilon(d_1, d_2) = \pm 1$*, and the sum is over non-ordered decompositions* $n = d_1d_2$ *such that* $d_1, d_2 > 0$ *and* $d_2 \equiv 1 \pmod 8$.

Proof. Writing equation (2.3.1) in terms of non-ordered decompositions, we have

$$\sum_{n=d_1d_2} P(d_1, d_2) = 2^{h_2(n)-\delta} Q(n),$$

where $\delta = 1$ if $n \equiv 1 \pmod 8$ and $\delta = 0$ otherwise. Here in the case $n \equiv 1 \pmod 8$, we have used the symmetry $P(d_1, d_2) = P(d_2, d_1)$. Apply Theorem 2.1. □

Finally, we are ready to derive Theorem 2.2.

Proof of Theorem 2.2. Since $\mathcal{L}(1) = 1$, the above lemma gives a recursive formula

$$\pm\mathcal{L}(n) = Q(n) - \sum_{\substack{n=d_1d_2 \\ d_2\equiv 1 \pmod 8,\ d_2>1}} \epsilon(d_1, d_2)\mathcal{L}(d_1)\mathcal{L}(d_2).$$

Here the sum is over non-ordered decompositions. This formula determines $\mathcal{L}(n)$ uniquely. In particular, $\mathcal{L}(n)$ is an integer.

Now we prove the congruence formula

$$\mathcal{L}(n) \equiv \sum_{\substack{n=d_0d_1\cdots d_\ell \\ d_i\equiv 1 \pmod 8,\ i>0 \\ d_i>1,\ i\geq 0}} \prod_i Q(d_i) \pmod 2.$$

It suffices to prove that the congruence formula (applied to every $Q(d_1)$ and $Q(d_2)$ below) satisfies the recursive formula

$$Q(n) \equiv \sum_{\substack{n=d_1d_2 \\ d_2\equiv 1 \pmod 8,\ d_2>0}} \mathcal{L}(d_1)\mathcal{L}(d_2) \pmod 2.$$

Namely, we need to check that

$$Q(n) \equiv \sum_{\substack{n=d_1d_2\\ d_2\equiv 1 \,(\mathrm{mod}\, 8),\ d_2>0}} \left(\sum_{\substack{d_1=d_0'd_1'\cdots d_{\ell'}'\\ d_j'\equiv 1\,(\mathrm{mod}\,8),\ j>0\\ d_j'>1,\ j\geq 0}} \prod_{j\geq 0} g(d_j')\right)\left(\sum_{\substack{d_2=d_0''d_1''\cdots d_{\ell''}''\\ d_k''\equiv 1\,(\mathrm{mod}\,8),\ k>0\\ d_k''>1,\ k\geq 0}} \prod_{k\geq 0} g(d_k'')\right) \pmod 2.$$

The right-hand side is a $\mathbb{Z}$-linear combination of

$$\prod_{j=0}^{\ell'} g(d_j') \prod_{k=0}^{\ell''} g(d_k'').$$

We consider the multiplicity of this term in the sum. Each appearance of such a term gives a partition

$$\{d_1', \cdots, d_{\ell'}', d_0'', \cdots, d_{\ell''}''\} = \{d_1', \cdots, d_{\ell'}'\} \coprod \{d_0'', \cdots, d_{\ell''}''\}.$$

If the set on the left-hand side is non-empty, the number of such partitions is even. Then the contribution of this set in the sum is zero modulo 2. Thus, we are only left with the empty set, which corresponds to the unique term $g(n)$ on the right. This proves the formula. □

Proof of Proposition 2.3. The proof easily follows from the explicit result in Theorem 2.6. In fact, take $K = K_n$ and $\chi = 1$ in the theorem. We see that the primitive test vector $f_n = \pi(g) f_0$ for some $g \in B_2^\times$, where

$$f_0 = \begin{cases} f_{\frac{i-j}{2}} + f_{\frac{j-k}{2}} + f_{\frac{k-i}{2}}, & \text{if } K_2 = \mathbb{Q}_2(\sqrt{-3}),\\ f_{i+j} = \frac{1}{2}\left(f_{\frac{i+j}{2}} + f_{\frac{i-j}{2}}\right), & \text{if } K_2 = \mathbb{Q}_2(\sqrt{-1}),\\ f_{\frac{i+j}{2}}, & \text{if } K_2 = \mathbb{Q}_2(\sqrt{-2m}) \text{ with } m \text{ odd.}\end{cases}$$

Note that the case $(K_2, \chi_2(\varpi)) = (\mathbb{Q}_2(\sqrt{-1}), -1)$ does not occur here. It is immediate that f_0 and f take odd values everywhere in the first and the third cases.

Assume that we are in the case $K_2 = \mathbb{Q}_2(\sqrt{-1})$. By Theorem 2.4, $\chi_0 f_{\frac{i+j}{2}} = f_{\frac{i-j}{2}}$. For any $h \in \widehat{B}^\times$, we have

$$f_n(h^2) = f_0(h^2 g) = \frac{1}{2} f_{\frac{i+j}{2}}(h^2 g)(1 + \chi_0(h^2 g)) = f_{\frac{i+j}{2}}(h^2 g) = \pm 1,$$

which is odd. Here we have used the fact $\chi_0(g) = 1$, which has been treated in the proof of Lemma 2.8.

3. Quadratic points and genus points.

This section treats $\mathcal{L}(n)$ for $n \equiv 5, 6, 7 \pmod 8$. The goal is to prove Theorem 1.4. We assume $n \equiv 5, 6, 7 \pmod 8$ throughout this section. The method is to construct rational points using the tower $X = \lim_U X_U$ of modular curves X_U.

3.1. Quadratic points and genus points.

In the following, we will mainly work on the elliptic curve $A : 2y^2 = x^3 + x$ (instead of $E : y^2 = x^3 - x$), which is isomorphic to $(X_0(32), \infty)$. Fix an identification $i_0 : (X_0(32), \infty) \to A$. We will introduce a morphism $f_n : X_V \to A$ from a certain modular curve X_V to A, and use this morphism to produce Heegner points on A.

Test vector. Recall that the open compact subgroup $U_0(32)$ of $\mathrm{GL}_2(\widehat{\mathbb{Q}})$ is given by

$$U_0(32)=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in \mathrm{GL}_2(\widehat{\mathbb{Z}}):32|c\right\}.$$

Define another open compact subgroup

$$U=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in U_0(32):4|(a-d)\right\}.$$

Then U is a normal subgroup of $U_0(32)$ of index two.

Denote by $f_0:X_U\to A$ the natural projection map $X_U\to X_0(32)$. It is finite and étale of degree 2. Note that the geometrically connected components of X_U are parametrized by $\mathrm{Spec}\,\mathbb{Q}(i)$. Then it is easy to figure out that $X_U\cong X_0(32)_{\mathbb{Q}(i)}$ over $\mathbb{Q}$, and under this identification f_0 is the natural map by the base change. Then

$$\mathrm{Aut}_{\mathbb{Q}}(X_U)=\mathrm{Aut}_{\mathbb{Q}(i)}(X_0(32)_{\mathbb{Q}(i)})\rtimes\{1,\epsilon\},$$

where ϵ is the Hecke operator given by $\begin{pmatrix}1&\\&-1\end{pmatrix}$, which is also the automorphism coming from the non-trivial automorphism of $\mathrm{Spec}\,\mathbb{Q}(i)$.

For $n\equiv 7\ (\mathrm{mod}\,8)$, let $f_n:X_0(32)\to A$ be the identity map $i_0:X_0(32)\to A$. For $n\equiv 5,6\ (\mathrm{mod}\,8)$, define $f_n:X_U\to A$ by

$$f_n:=\begin{cases}f_0-f_0\circ[i], & \text{if } n\equiv 5\ (\mathrm{mod}\,8),\\ f_0\circ[i], & \text{if } n\equiv 6\ (\mathrm{mod}\,8).\end{cases}$$

Denote $K_n=\mathbb{Q}(\sqrt{-n})$ as before. Embed K_n into $M_2(\mathbb{Q})$ by

$$\sqrt{-n}\longmapsto\begin{pmatrix}-1&1/4\\-4(n+1)&1\end{pmatrix},\qquad\begin{pmatrix}&1/4\\-4n&\end{pmatrix},\qquad\begin{pmatrix}\delta&2\\-(n+\delta^2)/2&-\delta\end{pmatrix},$$

according to $n\equiv 5,6,7\ (\mathrm{mod}\,8)$ respectively. Here δ is an integer such that $\delta^2\equiv -n\ (\mathrm{mod}\,128)$ in the case $n\equiv 7\ (\mathrm{mod}\,8)$.

The embeddings look arbitrary, but they are chosen on purpose. For $n\equiv 5,6\ (\mathrm{mod}\,8)$, the embeddings make $K_{n,2}^\times$ normalize U_2 in $\mathrm{GL}_2(\mathbb{Q}_2)$ at the place 2, which is the basis of our treatment. For $n\equiv 7\ (\mathrm{mod}\,8)$, the embedding gives $\widehat{O}_K^\times\subset U_0(32)$, which makes the easiest calculation.

Similarly, the choices of f_n seem artificial and technical here. However, they are obtained by some prescribed representation-theoretical properties below. Following [33, §1.2], consider the representation

$$\pi=\mathrm{Hom}^0_\infty(X,A)=\varinjlim_V\mathrm{Hom}^0_\infty(X_V,A)$$

of $\mathrm{GL}_2(\widehat{\mathbb{Q}})$. Here for any open compact subgroup V of $\mathrm{GL}_2(\widehat{\mathbb{Q}})$,

$$\mathrm{Hom}^0_\infty(X_V,A)=\mathrm{Hom}_\infty(X_V,A)\otimes_{\mathbb{Z}}\mathbb{Q},$$

where

$$\mathrm{Hom}_\infty(X_V,A)=\{f\in\mathrm{Hom}(X_V,A):\ f(\infty)\in A(\overline{\mathbb{Q}})_{\mathrm{tor}}\}.$$

Here ∞ denotes the cusp at infinity of X_V.

Proposition 3.1.

(1) *If $n \equiv 5, 6 \pmod 8$, the space $\pi^{\mathrm{GL}_2(\widehat{\mathbb{Z}}^{(2)})\cdot K_{n,2}^\times}$ is one-dimensional and contains f_n.*
(2) *If $n \equiv 7 \pmod 8$, the space $\pi^{U_0(32)}$ is one-dimensional and contains f_n.*

The proposition (will be proved in next section) explains that f_n is an explicit vector in a one-dimensional space in the framework of the multiplicity one theorem of Tunnell [28] and Saito [24]. See Theorem A.1 and Corollary A.2. One can also define an integral structure $\pi_{\mathbb{Z}}$ of π as the subgroup of elements of π coming from $\mathrm{Hom}_\infty(X_V, A)$ for some V. Then one can consider the primitivity of f_n under this integral structure as in §2. However, this is too involved in the current setting, so we will only consider the behavior of f_n in the rational structure π.

CM Points. Note that we have chosen an explicit embedding of K_n in $M_2(\mathbb{Q})$, which induces an action of $K_n^\times$ on the upper half plane $\mathcal{H}$. Let

$$P_n = [h, 1] \in X_U(\mathbb{C})$$

be the CM point, where $h \in \mathcal{H}^{K_n^\times}$ is the unique fixed point of $K_n^\times$ in $\mathcal{H}$. Let

$$z_n = f_n(P_n) \in A(K_n^{\mathrm{ab}}).$$

Note that z_n is not necessarily defined over the Hilbert class field H_n of K_n. Denote by $H_n' = H_n(z_n)$ the extension of H_n generated by the residue field of z_n. The following result is a precise description of the field of definition of z_n. In the following, denote by

$$\sigma : K_n^\times \backslash \widehat{K}_n^\times \longrightarrow \mathrm{Gal}(K_n^{\mathrm{ab}}/K_n)$$

the geometric Artin map, normalized by sending the uniformizers to the geometric Frobenii. So it is the reciprocal of the usual Artin map.

Proposition 3.2.
(1) *Assume that $n \equiv 5 \pmod 8$. Then $\mathrm{Gal}(H_n'/H_n) \simeq \mathbb{Z}/2\mathbb{Z}$ is generated by σ_ϖ^2. Here $\varpi = (\sqrt{-n} - 1)_2 \in K_{n,2}^\times$. The field $H_n'(\sqrt{2})$ is the ring class field of conductor 4 over K_n. The Galois group $\mathrm{Gal}(H_n'(\sqrt{2})/H_n) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ is generated by $\sigma_{1+2\varpi}$ and σ_ϖ^2, and H_n' is the subfield of $H_n'(\sqrt{2})$ fixed by $\sigma_{1+2\varpi}$.*
(2) *Assume that $n \equiv 6 \pmod 8$. Then $\mathrm{Gal}(H_n'/H_n) \simeq \mathbb{Z}/4\mathbb{Z}$ is generated by $\sigma_{1+\varpi}$. Here $\varpi = (\sqrt{-n})_2 \in K_{n,2}^\times$. The subfield of H_n' fixed by $\sigma_{1+\varpi}^2$ is $H_n(i)$. The field H_n' is exactly the ring class field of conductor 4 over K_n.*
(3) *Assume that $n \equiv 7 \pmod 8$. Then $H_n' = H_n$.*
(4) *For any $n \equiv 5, 6, 7 \pmod 8$, $2z_n$ is defined over H_n.*

The Proposition 3.2 will be proved in next section. Denote $K_n' = K_n, K_n(i), K_n$ according to $n \equiv 5, 6, 7 \pmod 8$ respectively. Set $\mathrm{Cl}_n = \mathrm{Gal}(H_n/K_n)$ and $\mathrm{Cl}_n' = \mathrm{Gal}(H_n'/K_n')$. Let σ be the unique order-two element of $\mathrm{Gal}(H_n'/H_n)$ in the case $n \equiv 5, 6 \pmod 8$, and set $\sigma = 1$ in the case $n \equiv 7 \pmod 8$. Then the natural map $\mathrm{Cl}_n' \to \mathrm{Cl}_n$ induces two isomorphisms

$$\mathrm{Cl}_n'/\langle\sigma\rangle \cong \mathrm{Cl}_n, \quad (2\mathrm{Cl}_n')/\langle\sigma\rangle \cong 2\mathrm{Cl}_n.$$

The least obvious case is the second isomorphism for $n \equiv 6 \pmod 8$. For that, it suffices to check that $\sigma = \sigma_{1+\varpi}^2$ lies in $2\mathrm{Cl}_n'$. Note that $\sigma_{1+\varpi} \notin \mathrm{Cl}_n'$, but we use the relations $\sigma = (\sigma_{1+\varpi}\sigma_\varpi)^2$ and $\sigma_{1+\varpi}\sigma_\varpi \in \mathrm{Cl}_n'$ instead. In fact, an easy calculation shows $\sigma_\varpi^2 = 1$ (on H_n') and $\sigma_\varpi(i) = -i$, which give the new relations.

Quadratic point. Fix a set $\Phi \subset \mathrm{Cl}'_n$ of representatives of $\mathrm{Cl}'_n/\langle\sigma\rangle \cong \mathrm{Cl}_n$. Let $\chi : \mathrm{Cl}_n \to \{\pm 1\}$ be a character. Define the quadratic point P_χ associated to χ by

$$P_\chi := \sum_{t\in\Phi} f_n(P_n)^t \chi(t) \in A(H'_n).$$

Here χ is also viewed as a function on Φ via the bijection $\Phi \to \mathrm{Cl}_n$.

To give a formula for P_χ, we need to describe another algebraic point on the elliptic curve. Recall that $\mathcal{L}(n)$ and $\rho(n)$ are defined in the introduction of this paper. We will see that $\mathcal{L}(n)$ is a rational number. Define

$$\mathcal{P}(n) := 2^{-1-\rho(n)}\mathcal{L}(n)\alpha_n \in A(K_n)^- \otimes_{\mathbb{Z}} \mathbb{Q},$$

where

$$A(K_n)^- := \{\alpha \in A(K_n) : \bar{\alpha} = -\alpha\} \ \subset \ A(K_n),$$

and $\alpha_n \in A(K_n)^-$ is any point which generates the free part $A(K_n)^-/A(K_n)^-_{\mathrm{tor}}$ if $\mathcal{L}(n) \neq 0$. Note that $\mathcal{P}(n) = 0$ if $\mathcal{L}(n) = 0$. The following theorem will be proved in appendix.

Theorem 3.3 (Gross-Zagier formula). *Let $\chi : \mathrm{Cl}_n \to \{\pm 1\}$ be a character. The point P_χ is non-torsion only if χ is of the form*

$$\chi_{d_0,d_1}, \quad n = d_0 d_1,\ 0 < d_0 \equiv 5,6,7 \pmod 8),\ 0 < d_1 \equiv 1,2,3 \pmod 8),$$

where χ_{d_0,d_1} is the unique Hecke character over K_n associated to the extension $K_n(\sqrt{d_1})$ for $n \equiv 5,6 \pmod 8)$ or $K_n(\sqrt{d_1^*})$ for $n \equiv 7 \pmod 8)$. Here $d_1^* = (-1)^{(d_1-1)/2}d_1$ as before.

In that case, in the vector space $A(H'_n(i)) \otimes_{\mathbb{Z}} \mathbb{Q} = A(H'_n(i)) \otimes_{\mathbb{Z}[i]} \mathbb{Q}[i]$,

$$P_\chi = \epsilon(d_0,d_1) 2^{h_2(n)} \mathcal{L}(d_1)\mathcal{P}(d_0),$$

where $\epsilon(d_0,d_1) = \pm i$ if $(d_0,d_1) \equiv (5,3) \pmod 8)$ and $\epsilon(d_0,d_1) = \pm 1$ otherwise.

Genus point. Set $\Phi_0 = \Phi \cap (2\mathrm{Cl}'_n)$ as a subset of Cl'_n. Then $\Phi_0 \subset 2\mathrm{Cl}'_n$ is a set of representatives of $(2\mathrm{Cl}'_n)/\langle\sigma\rangle \cong 2\mathrm{Cl}_n$ in $2\mathrm{Cl}'_n$. Define

$$Z(n) := \sum_{t\in\Phi_0} f_n(P_n)^t \in A(H'_n).$$

To compare $Z(d_0)$ for different divisors d_0 of n, we introduce the composite field

$$\mathbb{H}'_n := L_n(i) \cdot \prod_{\substack{d_0|n,\ d_0>0 \\ d_0\equiv 5,6 \pmod 8)}} H'_{d_0} \subset \overline{\mathbb{Q}}.$$

Here $L_n(i) = \mathbb{Q}(i, \sqrt{d} : d|n)$. The field seems to be very large, but we will see that $A(\mathbb{H}'_n)_{\mathrm{tor}} \subset A[4]$ in Lemma 3.18, which is a key property in our treatment. Note that $A(\mathbb{H}'_n)$ is a $\mathbb{Z}[i]$-module. Define $P(n) \in A(\mathbb{H}'_n)$ inductively by

$$P(n) := Z(n) - \sum_{\substack{n=d_0d_1 \\ d_0\equiv 5,6,7 \pmod 8) \\ d_1\equiv 1,2,3 \pmod 8),\ d_1>1}} \epsilon(d_0,d_1)\mathcal{L}(d_1)P(d_0),$$

where $\epsilon(d_0, d_1) \in \mu_4$ is as in Theorem 3.3. Note that $\mathcal{L}(d_1) \in \mathbb{Z}$ by Theorem 1.1. By definition, it is easy to verify the following congruence formula.

Proposition 3.4. *In $A(\mathbb{H}'_n)$,*

$$P(n) \equiv \sum_{\substack{n=d_0d_1\cdots d_\ell \\ d_0\equiv 5,6,7 \pmod 8 \\ d_1\equiv 1,2,3 \pmod 8 \\ d_i\equiv 1 \pmod 8,\ i>1}} \epsilon(d_0,d_1)\left(\prod_{i\geq 1} g(d_i)\right) Z(d_0)$$

$$+\, i \sum_{\substack{n=d_0d_1\cdots d_\ell \\ (d_0,d_1,d_2)\equiv (5,3,2) \pmod 8 \\ d_i\equiv 1 \pmod 8,\ i>2}} \left(\prod_{i\geq 1} g(d_i)\right) Z(d_0) \qquad \bmod\ 2A(\mathbb{H}'_n).$$

The main result of this section is as follows, which is an enhanced version of Theorem 1.4.

Theorem 3.5. *The vector $\mathcal{P}(n) \in A(K_n)^- \otimes_{\mathbb{Z}} \mathbb{Q}$ is represented by the point $P(n) \in A(\mathbb{H}'_n)$ in the sense that they are equal in $A(\mathbb{H}'_n) \otimes_{\mathbb{Z}} \mathbb{Q}$. Moreover,*

(1) *The image of $2P(n)$ under any 2-isogeny from A to E belongs to $E(K_n)^-$, i.e. $\mathcal{L}(n)$ is integral.*

(2) *Assume that $P(n) \in A(K_n)^- + A[4]$, i.e. $2^{-\rho(n)}\mathcal{L}(n)$ is even. If $n \equiv 5, 7 \pmod 8$, then*

$$\sum_{\substack{n=d_0\cdots d_\ell \\ d_i\equiv 1 \pmod 8,\ i>0}} \prod_i g(d_i) \equiv \sum_{\substack{n=d_0\cdots d_\ell, \\ d_0\equiv 5,6,7 \pmod 8 \\ d_1\equiv 1,2,3 \pmod 8 \\ d_i\equiv 1 \pmod 8,\ i>1}} \prod_i g(d_i) \equiv 0 \pmod 2.$$

If $n \equiv 6 \pmod 8$, then

$$\sum_{\substack{n=d_0\cdots d_\ell, \\ d_0\equiv 5,6,7 \pmod 8 \\ d_1\equiv 1,2,3 \pmod 8 \\ d_i\equiv 1 \pmod 8,\ i>1}} \prod_i g(d_i) \equiv 0 \pmod 2.$$

Theorem 3.3, Proposition 3.4 and Theorem 3.5 will be proved in section 3.3.

3.2. Test vectors. Recall that in Proposition 3.2 we have described the field $H'_n = H_n(z_n)$. The major goal of this section is to prove some results about Galois actions on z_n. We will also prove Proposition 3.1 and Proposition 3.2.

To describe the results about Galois actions on z_n, we recall some basic facts about $X_0(32)$ and A, which are basic facts or results proved in [26].

(1) There is an analytic isomorphism

$$\tau : \mathbb{C}/(1+i)\mathbb{Z}[i] \longrightarrow A(\mathbb{C}).$$

The map τ is unique up to multiplication by $\mu_4 = \{\pm 1, \pm i\}$. We can adjust τ such that $\mathbb{R}/2\mathbb{Z}$ maps onto $A(\mathbb{R})$ and

$$A[2^\infty] = \mathbb{Q}_2(i)/(1+i)\mathbb{Z}_2[i] \subset \mathbb{Q}(i)/(1+i)\mathbb{Z}[i] = A(\mathbb{C})_{\mathrm{tor}}.$$

(2) Under the uniformization τ, the Galois group $G_{\mathbb{Q}} = G_{\mathbb{Q}(i)} \rtimes \{1, c\}$ acts on $A[2^\infty] = \mathbb{Q}_2(i)/(1+i)\mathbb{Z}_2[i]$ as follows. The induced action of c on $\mathbb{Q}_2(i)/(1+i)\mathbb{Z}[i]$ is still given by the conjugation $i \mapsto -i$, and the induced action of $G_{\mathbb{Q}(i)}$ on $\mathbb{Q}_2(i)/(1+i)\mathbb{Z}[i]$ is given by multiplying by the composition

$$\begin{aligned} G_{\mathbb{Q}(i)} \to \mathrm{Gal}(\mathbb{Q}(i)^{\mathrm{ab}}/\mathbb{Q}(i)) &\xrightarrow{\sigma_{\mathbb{Q}(i)}^{-1}} \mathbb{Q}(i)^\times \backslash \widehat{\mathbb{Q}(i)}^\times \\ &\cong (1 + (1+i)^3 \widehat{\mathbb{Z}[i]})^\times \to (1 + (1+i)^3 \mathbb{Z}_2[i])^\times, \end{aligned}$$

where $\sigma_{\mathbb{Q}(i)}$ denotes the Artin map and the last map is the natural projection.

(3) The identification $i_0 : X_0(32) \to A$ (mapping ∞ to 0) identifies the set $\mathcal{S} = \Gamma_0(32)\backslash\mathbb{P}^1(\mathbb{Q})$ of cusps with $A[(1+i)^3] = A(\mathbb{Q}(i))$. Replacing τ by $-\tau$ if necessary, we can (and we will) assume that the induced bijection

$$\tau : \frac{1}{2}\mathbb{Z}[i]/(1+i)\mathbb{Z}[i] \longrightarrow A[(1+i)^3] = \Gamma_0(32)\backslash\mathbb{P}^1(\mathbb{Q})$$

gives

$$\tau(0) = [\infty], \qquad \tau(1/2) = [0], \qquad \tau(-1/2) = [1/2],$$

$$\tau(1) = [1/16], \qquad \tau(\pm i/2) = [\pm 1/4], \qquad \tau((1 \pm i)/2) = [\pm 1/8].$$

Now we are ready to state the main result of this subsection.

Theorem 3.6. *Resume the notations in Proposition 3.2. The following are true:*

(1) *Assume that $n \equiv 5 \pmod 8$. Then*

$$z_n^{\sigma_\varpi} = z_n + \tau(\frac{1+i}{2}), \qquad z_n^{\sigma_{1+2\varpi}} = z_n, \qquad \bar{z}_n = -z_n + \tau(1).$$

Thus $z_n^{\sigma_{\varpi^2/2}} = z_n^{\sigma_{\varpi^2}} = z_n + \tau(1)$.

(2) *Assume that $n \equiv 6 \pmod 8$. Then*

$$z_n^{\sigma_\varpi} = z_n + \tau(-i/2), \qquad z_n^{\sigma_{1+\varpi}} = z_n + \tau(\frac{1-i}{2}), \qquad \bar{z}_n = -z_n.$$

Thus $z_n^{\sigma_{1+\varpi}^2} = z_n + \tau(1)$.

(3) *Assume that $n \equiv 7 \pmod 8$. Let v_2 and v_2' be the two places of K_n above 2 such that $v_2(\sqrt{-n} - \delta) \geq 6$. Let $\varpi \in K_{n,2}$ be an element with $v_2(\varpi) = 1$ and $v_2'(\varpi) = 0$. Then*

$$\bar{z}_n + z_n^{\sigma_{\varpi^5}} = \tau(1/2).$$

Here $\bar{z}_n$ denotes the complex conjugate of z_n. The results will be treated case by case in the following. For simplicity, we write K for K_n (so that K_2 means the local field $K_{n,2}$ of K_n at 2).

Case $n \equiv 5 \pmod 8$. In this case, $f_n : X_U \to A$ is given by $f_n = f_0 - f_0 \circ [i]$, and the embedding of K into $M_2(\mathbb{Q})$ is given by

$$\sqrt{-n} \longmapsto \begin{pmatrix} -1 & 1/4 \\ -4(n+1) & 1 \end{pmatrix}.$$

The embedding gives $(\widehat{\mathbb{Z}} + 4\widehat{O}_K)^\times \subset U$.

Lemma 3.7. *Assume $n \equiv 5 \pmod 8$.*

(1) *The quotient* $K_2^\times/\mathbb{Q}_2^\times(1+4O_{K,2})$ *is isomorphic to* $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, *and generated by the order-four element* $\varpi=(\sqrt{-n}-1)_2$ *and the order-two element* $1+2\varpi$.
(2) *The multiplicative group* $K_2^\times$ *normalizes* U_2.

Proof. We first check (1). Note that K_2 is ramified over $\mathbb{Q}_2$. Then $\mathbb{Q}_2^\times O_{K,2}^\times$ has index two in $K_2^\times$. Then $K_2^\times/\mathbb{Q}_2^\times(1+4O_{K,2})$ has an index-two subgroup

$$\mathbb{Q}_2^\times O_{K,2}^\times/\mathbb{Q}_2^\times(1+4O_{K,2})=O_{K,2}^\times/\mathbb{Z}_2^\times(1+4O_{K,2})=(O_{K,2}/4O_{K,2})^\times/\{\pm1\}\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}.$$

It follows that $K_2^\times/\mathbb{Q}_2^\times(1+4O_{K,2})$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Now it is easy to check that ϖ and $1+2\varpi$ generate the group.

For (2), since $1+4O_{K,2}\subset U$, we see that $\mathbb{Q}_2^\times(1+4O_{K,2})$ normalizes U_2. By (1), it suffices to check that ϖ and $1+2\varpi$ normalize U_2, which can be done by explicit calculations. □

By the lemma, $K_2^\times$ normalizes U_2, and thus it acts on X_U by the right multiplication. The subgroup $\mathbb{Q}_2^\times(1+4O_{K_n,2})$ acts trivially and induces a homomorphism

$$K_2^\times/\mathbb{Q}_2^\times(1+4O_{K_n,2})\longrightarrow\mathrm{Aut}_{\mathbb{Q}}(X_U).$$

We will describe this homomorphism explicitly.

The following result contains a lot of identities in

$$\mathrm{Aut}_{\mathbb{Q}}(X_U)=\mathrm{Aut}_{\mathbb{Q}(i)}(X_0(32)_{\mathbb{Q}(i)})\rtimes\{1,\epsilon\}\simeq(A(\mathbb{Q}(i))\rtimes\mu_4)\rtimes\{1,\epsilon\}.$$

Here $\epsilon=\begin{pmatrix}1&\\&-1\end{pmatrix}\in\mathrm{GL}_2(\mathbb{Q})$ also normalizes U, and its Hecke action on X_U gives the non-trivial element of $\mathrm{Gal}(X_U/X_0(32))$. In particular, ϵ acts on $\mathrm{Aut}_{\mathbb{Q}(i)}(X_0(32)_{\mathbb{Q}(i)})$ by sending i to $-i$. Recall that we have also identified

$$A(\mathbb{Q}(i))=\frac{1}{2}\mathbb{Z}[i]/(1+i)\mathbb{Z}[i]$$

with the set $\mathcal{S}$ of cusps of $X_0(32)$.

PROPOSITION 3.8. *Assume* $n\equiv5\,(\mathrm{mod}\,8)$.
(1) *For any* $Q\in X_U(\mathbb{C})$,

$$Q^\varpi=[i]Q^\epsilon+\tau(\frac{1}{2}),\qquad Q^{1+2\varpi}=Q+\tau(1).$$

(2) *The order-two element* $j=\begin{pmatrix}1&0\\8&-1\end{pmatrix}\in\mathrm{GL}_2(\mathbb{Q})$ *normalizes* $K^\times$ *such that* $jxj=\overline{x}$ *for all* $x\in K^\times$ *and normalizes* U *with the induced action on* X_U *given by*

$$Q^j=[-i]Q^\epsilon+\tau(\frac{1+i}{2}),\quad\forall\,Q\in X_U(\mathbb{C}).$$

Proof. The right translation by an element $g\in\mathrm{GL}_2(\mathbb{A}_f)$ switches the two geometric components of X_U if and only if the image of g under the composition

$$\mathrm{GL}_2(\widehat{\mathbb{Q}})\xrightarrow{\det}\widehat{\mathbb{Q}}^\times=\mathbb{Q}_+^\times\cdot\widehat{\mathbb{Z}}^\times\longrightarrow(\mathbb{Z}_2/4\mathbb{Z}_2)^\times\cong\{\pm1\}$$

is -1. For example, all $\epsilon = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $j = \begin{pmatrix} 1 & 0 \\ 8 & -1 \end{pmatrix}$, and $\varpi = \begin{pmatrix} -2 & 1/4 \\ -4(n+1) & 0 \end{pmatrix}$ are such elements, but $1 + 2\varpi$ is not.

Hence, the actions of $\varpi\epsilon$, $1 + 2\varpi$ and $j\epsilon$ take the form

$$Q^{\varpi\epsilon} = \alpha Q + R, \quad Q^{1+2\varpi} = \beta Q + S, \quad Q^{j\epsilon} = \gamma Q + T$$

where $\alpha, \beta, \gamma \in \mu_4$ and $R, S, T \in \mathcal{S}$ are cusps of $X_0(32)$. Here the right sides belong to

$$\mathrm{Aut}_{\mathbb{Q}(i)}(X_0(32)_{\mathbb{Q}(i)}) = \mathrm{Aut}(X_U/\mathbb{Q}(i)) \subset \mathrm{Aut}_{\mathbb{Q}}(X_U).$$

To compute R, S, T, we take $Q = [\infty]$. In terms of the complex uniformization

$$X_0(32)(\mathbb{C}) = \mathrm{GL}_2(\mathbb{Q})_+ \backslash (\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})) \times \mathrm{GL}_2(\widehat{\mathbb{Q}})/U_0(32),$$

we have

$$R = [\infty, \varpi\epsilon], \quad S = [\infty, 1 + 2\varpi], \quad T = [\infty, j\epsilon].$$

We need to convert them to expressions of the form $[\theta] = [\theta, 1]$ with $\theta \in \mathbb{P}^1(\mathbb{Q})$. By the complex uniformization,

$$\begin{aligned} \mathcal{S} &= \mathrm{GL}_2(\mathbb{Q})_+ \backslash \mathbb{P}^1(\mathbb{Q}) \times \mathrm{GL}_2(\widehat{\mathbb{Q}})/U_0(32) = P(\mathbb{Q})_+ \backslash \mathrm{GL}_2(\widehat{\mathbb{Q}})/U_0(32) \\ &= P(\mathbb{Q})_+ \backslash P(\widehat{\mathbb{Q}}) \cdot \mathrm{GL}_2(\widehat{\mathbb{Z}})/U_0(32) = N(\mathbb{Z}_2) \backslash \mathrm{GL}_2(\mathbb{Z}_2)/U_0(32)_2. \end{aligned}$$

Here P (resp. N) stands for the parabolic (resp. unipotent) subgroup of upper triangles of GL_2, respectively. For the truth of the last identity, we refer to [33, Lemma 4.6.3 (2)]. We have decompositions in $\mathrm{GL}_2(\mathbb{Q}_2)$ as follows:

$$\begin{aligned} \varpi\epsilon &= \begin{pmatrix} 1/4 & 0 \\ 0 & 8 \end{pmatrix} \begin{pmatrix} -8 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -(n+1)/2 & 0 \\ 4(n+3) & 1 \end{pmatrix}, \\ 1 + 2\varpi &= \begin{pmatrix} 1 & 1/2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -16 & 1 \end{pmatrix} \begin{pmatrix} 4n+1 & 0 \\ 8(7n+1) & 1 \end{pmatrix}, \\ j\epsilon &= \begin{pmatrix} 1 & 0 \\ 8 & 1 \end{pmatrix}. \end{aligned}$$

It follows that

$$R = \left[\infty, \begin{pmatrix} -8 & -1 \\ 1 & 0 \end{pmatrix}_2\right] = \left[\begin{pmatrix} -8 & -1 \\ 1 & 0 \end{pmatrix}^{-1} \infty, 1\right] = [0] = \tau(1/2).$$

Similarly, $S = [1/16] = \tau(1)$ and $T = [-1/8] = \tau((1-i)/2)$.

To find α, β, γ, we only need check the action on the cusp $[0] = \left[\infty, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right]$. We have decompositions:

$$\begin{aligned} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \varpi\epsilon &= \begin{pmatrix} 8 & 0 \\ 0 & 1/4 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 8 & 1 \end{pmatrix} \begin{pmatrix} (n+1)/2 & 0 \\ -4(n+3) & -1 \end{pmatrix}, \\ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} (1 + 2\varpi) &= \begin{pmatrix} -2 & +1 \\ 0 & -1/2 \end{pmatrix} \begin{pmatrix} 7 & -3 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 4n-17 & 3 \\ 8(n-5) & 7 \end{pmatrix}, \\ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} j\epsilon &= \begin{pmatrix} 8 & 1 \\ -1 & 0 \end{pmatrix}. \end{aligned}$$

It follows that

$$[0]^{\varpi\epsilon}=[-1/8]=\tau((1-i)/2),\quad [0]^{1+2\varpi}=[1/2]=\tau(-1/2),\quad [0]^{j\epsilon}=[0]=\tau(1/2).$$

We then have the equations

$$\begin{aligned}\tau((1-i)/2)&=\alpha\tau(1/2)+\tau(1/2),\\ \tau(-1/2)&=\beta\tau(1/2)+\tau(1),\\ \tau(1/2)&=\gamma\tau(1/2)+\tau((1-i)/2),\end{aligned}$$

which give $\alpha=-i$, $\beta=1$ and $\gamma=i$.

Therefore, we have

$$Q^{\varpi\epsilon}=[-i]Q+\tau(1/2),\qquad Q^{1+2\varpi}=Q+\tau(1),\quad Q^{j\epsilon}=[i]Q+\tau(\frac{1-i}{2}).$$

For the first and the the third equations, we take a further ϵ-action on both sides. Then

$$Q^{\varpi}=([-i]Q+\tau(1/2))^{\epsilon}=[i](Q^{\epsilon})+\tau(1/2)$$

and

$$Q^{j}=([i]Q+\tau(\frac{1-i}{2}))^{\epsilon}=[-i](Q^{\epsilon})+\tau(\frac{1+i}{2}).$$

It finishes the proof. □

The map $K_2^{\times}\to \mathrm{Aut}(X_U)$ induces an action of $K_2^{\times}$ on $\mathrm{Hom}(X_U,A)$. Still use π to denote this action. Now it is easy to have the action on $f_n=f_0\circ[1-i]$.

Corollary 3.9. *In* $\mathrm{Hom}(X_U,A)$,

$$\pi(\varpi)f_n=f_n+\tau(\frac{1+i}{2}),\qquad \pi(1+2\varpi)f_n=f_n.$$

Proof. For any $Q\in X_U(\mathbb{C})$,

$$(\pi(\varpi)f_n)(Q)=f_0([1-i]Q^{\varpi}).$$

By the proposition,

$$[1-i]Q^{\varpi}=[1-i]([i]Q^{\epsilon}+\tau(1/2))=[1+i]Q^{\epsilon}+\tau(\frac{1-i}{2})=([1-i]Q+\tau(\frac{1+i}{2}))^{\epsilon}.$$

Note that f_0 is invariant under ϵ. Thus

$$(\pi(\varpi)f_n)(Q)=f_0([1-i]Q+\tau(\frac{1+i}{2}))=f_0([1-i]Q)+\tau(\frac{1+i}{2})=f_n(Q)+\tau(\frac{1+i}{2}).$$

The second equality is proved similarly. □

The corollary is an integral version of Lemma 3.1 for $n\equiv 5\,(\mathrm{mod}\,8)$. Now f_n lies in the space $\pi^{\mathrm{GL}_2(\widehat{\mathbb{Z}}^{(2)})\cdot K_2^{\times}}\simeq\pi_2^{K_2^{\times}}$, which is one-dimensional by Theorem A.1 and Theorem A.2.

Now we are ready to prove Theorem 3.6 for $n \equiv 5 \pmod 8$, i.e.,

$$z_n^{\sigma_\varpi} = z_n + \tau(\frac{1+i}{2}), \qquad z_n^{\sigma_{1+2\varpi}} = z_n, \qquad \bar{z}_n = -z_n + \tau(1).$$

For the first two equalities, the key is that the Galois action of $K_2^\times$ on P (via the Artin map σ) is the same as the Hecke action of $K_2^\times$, by the special form of $P_n = [h, 1]$. Then by Corollary 3.9,

$$z_n^{\sigma_\varpi} = f_n(P_n^{\sigma_\varpi}) = f_n(P_n^{\varpi}) = (\pi(\varpi)f_n)(P_n) = f_n(P_n) + \tau(\frac{1+i}{2}) = z_n + \tau(\frac{1+i}{2}).$$

The second equality is similarly obtained.

For the third equality, the Hecke action of the element j in Proposition 3.8 (2) gives the complex conjugation of $P_n = [h, 1]$ by the condition $jxj^{-1} = \overline{x}$ for all $x \in K^\times$. In fact,

$$\bar{P}_n = [\bar{h}, 1], \quad P_n^j = [h, j] = [j(h), 1].$$

It suffices to check $\bar{h} = j(h)$. Note that $\{h, \bar{h}\}$ is the set of fixed points of $K^\times$ in $\mathcal{H}^\pm$. By $jK^\times j = K^\times$, we see that $\{h, \bar{h}\} = \{j(h), j(\bar{h})\}$ as sets. Since $\det(j) = -1 < 0$, we have $j(h) \in \mathcal{H}^-$ and thus $j(h) = \bar{h}$.

Hence,

$$\bar{z}_n = f_n(\bar{P}_n) = f_n(P_n^j) = f_n([-i]P_n^\epsilon + \tau(\frac{1+i}{2})) = f_0([-1-i]P_n^\epsilon + \tau(1)).$$

By $[-1-i]P_n^\epsilon + \tau(1) = ([-1+i]P_n^\epsilon + \tau(1))^\epsilon$, we have

$$\bar{z}_n = f_0([-1+i]P_n + \tau(1)) = -f_0(P_n) + \tau(1) = -z_n + \tau(1).$$

This proves the theorem in the current case.

Finally, we prove Proposition 3.2 for $n \equiv 5 \pmod 8$. By the reciprocity law, the point P_n is defined over the abelian extension of K with Galois group $\widehat{K}^\times / K^\times(\widehat{K}^\times \cap U)$. It is easy to see $(\widehat{\mathbb{Z}} + 4\widehat{O}_K)^\times \subset U$. Then P_n is defined over the ring class field $H_{n,4}$ of K with Galois group $\widehat{K}^\times / K^\times(\widehat{\mathbb{Z}} + 4\widehat{O}_K)^\times$. We have

$$\begin{aligned}\mathrm{Gal}(H_{n,4}/H_n) &\cong K^\times \widehat{O}_K^\times / K^\times(\widehat{\mathbb{Z}} + 4\widehat{O}_K)^\times = \widehat{O}_K^\times / (\widehat{\mathbb{Z}} + 4\widehat{O}_K)^\times \\ &= O_{K,2}^\times / (\mathbb{Z}_2 + 4O_{K,2})^\times = O_{K,2}^\times / \mathbb{Z}_2^\times(1 + 4O_{K,2}) = (O_{K,2}/4O_{K,2})^\times / \{\pm 1\}.\end{aligned}$$

As in the proof of Lemma 3.7, the right-hand side is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and generated by $\frac{1}{2}\varpi^2$ and $1 + 2\varpi$. Consider $z_n = f_n(P_n)$ and $H_n' = H_n(z_n) \subset H_{n,4}$. By Theorem 3.6,

$$z_n^{\sigma_{\varpi^2/2}} = z_n + \tau(1), \qquad z_n^{\sigma_{1+2\varpi}} = z_n.$$

It follows that H_n' is the index-two subfield of $H_{n,4}$ fixed by $\sigma_{1+2\varpi}$. Note that $\sqrt{2} \in H_{n,4}$ but $\sqrt{2} \notin H_n'$ by $\sigma_{1+2\varpi}(\sqrt{2}) = -\sqrt{2}$. The equations also indicate that $2z_n$ is invariant under both $\sigma_{\varpi^2/2}$ and $\sigma_{1+2\varpi}$, and thus it is defined over H_n. The proposition is proved in this case.

Case $n \equiv 6 \pmod 8$**.** Now we consider the case $n \equiv 6 \pmod 8$. The exposition is very similar to the previous case $n \equiv 5 \pmod 8$, and the calculations are slightly simpler. We still follow the process of the previous case, but only sketch some of the proofs.

In this case, $f_n : X_U \to A$ is given by $f_n = f_0 \circ [i]$, and the embedding of K into $M_2(\mathbb{Q})$ is given by

$$\sqrt{-n} \longmapsto \begin{pmatrix} & 1/4 \\ -4n & \end{pmatrix}.$$

The embedding still gives $(\widehat{\mathbb{Z}} + 4\widehat{O}_K)^\times \subset U$.

Lemma 3.10. *Assume* $n \equiv 6 \pmod 8$.

1. *The quotient* $K_2^\times/\mathbb{Q}_2^\times(1+4O_{K,2})$ *is isomorphic to* $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, *and generated by the order-two element* $\varpi = (\sqrt{-n})_2$ *and the order-four element* $1+\varpi$.
2. *The multiplicative group* $K_2^\times$ *normalizes* U_2.

Proof. The proof is similar to that of Lemma 3.7. □

Now we describe the homomorphism

$$K_2^\times/\mathbb{Q}_2^\times(1+4O_{K_n,2}) \longrightarrow \mathrm{Aut}_{\mathbb{Q}}(X_U).$$

Proposition 3.11. *Assume* $n \equiv 6 \pmod 8$.

1. *For any* $Q \in X_U(\mathbb{C})$,

$$Q^\varpi = -Q^\epsilon + \tau(\frac{1}{2}), \quad Q^{1+\varpi} = -Q^\epsilon + \tau(\frac{1-i}{2}).$$

2. *The order-two element* $\epsilon = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})$ *normalizes* $K^\times$ *such that* $\epsilon x \epsilon = \overline{x}$ *for all* $x \in K^\times$.

Proof. Follow the strategy of Proposition 3.8. The Hecke operators $\varpi\epsilon$ and $(1+\varpi)\epsilon$ do not switch the two geometric components of X_U. We have the decompositions

$$\varpi\epsilon = \begin{pmatrix} 1/4 & 0 \\ 0 & 8 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} n/2 & 0 \\ 0 & -1 \end{pmatrix},$$
$$(1+\varpi)\epsilon = \begin{pmatrix} 1 & 1/4 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 8 & -1 \end{pmatrix}\begin{pmatrix} -(1+n) & 0 \\ -8(1+n/2) & 1 \end{pmatrix}.$$

It follows that $\varpi\epsilon$ and $(1+\varpi)\epsilon$ maps $[\infty]$ to $[0]$ and $[1/8]$, respectively. Thus their action on X_U takes the form

$$Q^{\varpi\epsilon} = \alpha Q + \tau(1/2), \quad Q^{(1+\varpi)\epsilon} = \beta Q + \tau((1+i)/2)$$

for some $\alpha, \beta \in \mu_4$. Use the decompositions

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\varpi\epsilon = \begin{pmatrix} -8 & 0 \\ 0 & -1/4 \end{pmatrix}\begin{pmatrix} n/2 & 0 \\ 0 & -1 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}(1+\varpi)\epsilon = \begin{pmatrix} 4 & -1 \\ 0 & 1/4 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix}\begin{pmatrix} -(1+n) & 0 \\ -8(1+n/2) & 1 \end{pmatrix}.$$

Setting $Q = [0] = \tau(1/2)$, we have the equations

$$\tau(0) = \alpha\tau(1/2) + \tau(1/2), \quad \tau(i/2) = \beta\tau(1/2) + \tau((1+i)/2).$$

It follows that $\alpha = -1$ and $\beta = -1$. Hence, we have

$$Q^{\varpi\epsilon} = -Q + \tau(\frac{1}{2}), \quad Q^{(1+\varpi)\epsilon} = -Q + \tau(\frac{1+i}{2}).$$

Further actions by ϵ give the results. □

We have the following integral version of Lemma 3.1 for $n \equiv 5 \pmod 8$.

Corollary 3.12. *Assume* $n \equiv 6 \pmod 8$. *In* $\mathrm{Hom}(X_U, A)$,

$$\pi(\varpi)f_n = f_n + \tau(-\frac{i}{2}), \qquad \pi(1+\varpi)f_n = f_n + \tau(\frac{1-i}{2}).$$

Proof. The proof is similar to that of Corollary 3.9. □

Now we can prove Theorem 3.6 and Proposition 3.2 for $n \equiv 6 \pmod 8$ similarly. For example, the proof of $\bar{z}_n = -z_n$ is given by:

$$\bar{z}_n = f_n(\bar{P}_n) = f_n(P_n^\epsilon) = f_0([i]P_n^\epsilon) = f_0(([-i]P_n)^\epsilon) = f_0([-i]P_n) = -z_n.$$

Case $n \equiv 7 \pmod 8$**.** Now we consider the case $n \equiv 7 \pmod 8$. Then 2 is split over K. It is the simplest case since $f_n : X_0(32) \to A$ is just the identity map $i_0 : X_0(32) \to A$. The theory does not involve the more complicated curve X_U. For example, Proposition 3.1 is true in this case since $\dim \pi^{U_0(32)} = 1$ by the newform theory.

The embedding of K into $M_2(\mathbb{Q})$ is given by

$$\sqrt{-n} \longmapsto \begin{pmatrix} \delta & 2 \\ -(n+\delta^2)/2 & -\delta \end{pmatrix},$$

where $\delta \in \mathbb{Z}$ satisfies $\delta^2 \equiv -n \pmod{128}$. It is easy to check that the embedding gives $\widehat{O}_K^\times \subset U_0(32)$. Then Proposition 3.2 is automatic in this case.

The following is devoted to prove Theorem 3.6 in this case. Recall from the theorem that v_2 and v_2' are the two places of K_n above 2 such that $v_2(\sqrt{-n} - \delta) \geq 6$, and that $\varpi \in K_{n,2}$ is an element with $v_2(\varpi) = 1$ and $v_2'(\varpi) = 0$.

Proposition 3.13. *Assume* $n \equiv 7 \pmod 8$. *Let*

$$W = \begin{pmatrix} 0 & 1 \\ -32 & 0 \end{pmatrix}, \qquad j = \begin{pmatrix} 1 & \\ -\delta & -1 \end{pmatrix}$$

be elements of $\mathrm{GL}_2(\mathbb{Q})$. *Then*

(1) *The element* W *normalizes* $U_0(32)$, *and*

$$Q^W = -Q + \tau(1/2), \qquad \forall\ Q \in X_0(32)(\mathbb{C}).$$

(2) *One has* $j^2 = 1$, $jxj = \bar{x}$ *for any* $x \in K$, *and* $j\varpi^5 \in W \cdot U_0(32)_2$. *Therefore,*

$$Q^{j\varpi^5} = -Q + \tau(1/2), \qquad \forall\ Q \in X_0(32)(\mathbb{C}).$$

Proof. For (1), consider the Atkin–Lehner operator $\pi(W)$. Note that $\pi(W)f_n = -f_n$ in the $\mathbb{Q}$-space π since A has root number 1. It follows that, in the $\mathbb{Z}$-module $\mathrm{Hom}(X_0(32), A)$, the sum $\pi(W)f_n + f_n$ is a torsion point of A. To figure out the torsion point, evaluate at $[\infty]$. We have

$$(\pi(W)f_n + f_n)([\infty]) = f_n([\infty]^W) + f_n([\infty]) = \tau(1/2).$$

This proves (1).

For (2), consider the $\mathbb{Q}_2$-algebra $K_2 \cong K_{v_2} \times K_{v_2'} = \mathbb{Q}_2 \times \mathbb{Q}_2$. Let $\alpha \in \mathbb{Z}_2^\times$ be such that

$$(\alpha, -\alpha) = \sqrt{-n} \longmapsto \begin{pmatrix} \delta & 2 \\ -(n+\delta^2)/2 & -\delta \end{pmatrix}.$$

Then $64|(\alpha - \delta)$ and $2\|(\alpha+\delta)$. We may take $\varpi = (2, 1)$. Then

$$\varpi^5 = (32, 1) = \frac{31}{2\alpha}(\alpha, -\alpha) + \frac{33}{2}(1, 1)$$

corresponds to the matrix

$$\frac{31}{2\alpha}\begin{pmatrix} \delta & 2 \\ -(n+\delta^2)/2 & -\delta \end{pmatrix} + \frac{33}{2}\begin{pmatrix} 1 & \\ & 1 \end{pmatrix} = \frac{1}{2\alpha}\begin{pmatrix} 31\delta + 33\alpha & 62 \\ -31(n+\delta^2)/2 & -31\delta + 33\alpha \end{pmatrix}.$$

It is now straight forward to check $W^{-1}j\varpi^5 \in U_0(32)$. □

Now it is easy to obtain Theorem 3.6 for $n \equiv 7 \pmod 8$ which asserts

$$\bar{z}_n + z_n^{\sigma_{\varpi^5}} = \tau(1/2).$$

In fact, the proposition gives

$$P_n^{j\varpi^5} = -P_n + \tau(1/2).$$

As before, j computes the complex conjugate of P_n. Then the above becomes

$$(\bar{P}_n)^{\varpi^5} = -P_n + \tau(1/2).$$

The Hecke action is defined over $\mathbb{Q}$ and thus commutes with the complex conjugation. This finishes the proof.

3.3. Proofs of Theorem 3.3, Proposition 3.4 and Theorem 3.5. In this section, we prove our main theorems in the case $n \equiv 5, 6, 7 \pmod 8$.

Proof of Theorem 3.3. We first prove the following result, which gives the first statement of the theorem.

LEMMA 3.14. *Let $\chi : \mathrm{Cl}_n \to \{\pm 1\}$ be a character satisfying the following conditions:*

(1) The root number of $L(A_{K_n}, \chi, s)$ is -1;

(2) If 2 is not split in K_n, then the 2-component $\chi_2 : K_{n,2}^\times \to \{\pm 1\}$ of χ is trivial. Then χ is exactly of the form

$$\chi_{d_0,d_1}, \qquad n = d_0 d_1,\ 0 < d_0 \equiv 5, 6, 7 \pmod 8),\ 0 < d_1 \equiv 1, 2, 3 \pmod 8),$$

where χ_{d_0,d_1} is the unique Hecke character over K_n associated to the extension $K_n(\sqrt{d_1})$ for $n \equiv 5, 6 \pmod 8$ and $K_n(\sqrt{d_1^*})$ for $n \equiv 7 \pmod 8$.

Proof. The character χ corresponds to an extension over K_n of degree dividing 2 and inside the genus field L_n of K_n, which must be of form $K_n(\sqrt{d}) = K_n(\sqrt{-n/d})$ for some integer $d|n$ with $\sqrt{d} \in L_n$.

First, the L-function $L(A_{K_n}, \chi, s) = L(A_d, s)L(A_{n/d}, s)$ has root number -1 if and only if exactly one element of $\{|d|,\ n/|d|\}$ is congruent to $1, 2, 3$ modulo 8 and the other one is congruent to $5, 6, 7$ modulo 8. Thus we may assume that the extension corresponding to χ is of the form $K_n(\sqrt{\pm d_1}) \subset L_n$, $0 < d_1 \equiv 1, 2, 3 \pmod 8$, such that $d_0 := n/d_1 \equiv 5, 6, 7 \pmod 8$.

If $n \equiv 7 \pmod 8$, then 2 is split in K and the second condition is empty. Note that $\sqrt{d_1^*} \in L_n$ but $\sqrt{-d_1^*} \notin L_n$. Thus χ is exactly of desired form.

If $n \equiv 5 \pmod 8$, then 2 is ramified in K_n. Both $\sqrt{d_1}$ and $\sqrt{-d_1}$ are in L_n. We have $(d_0, d_1) \equiv (5, 1), (7, 3) \pmod 8$. The restriction that χ_2 is trivial implies that the extension corresponding to χ is $K_n(\sqrt{d_1})$ in the first case or $K_n(\sqrt{-d_0})$ in the second case. Then $K_n(\sqrt{d_1})$ is a uniform way to write down the field.

If $n \equiv 6 \pmod 8$, then 2 is ramified in K_n. We have $(d_0, d_1) \equiv (6, 1), (7, 2) \pmod 8$. Then the extension corresponding to χ is $K_n(\sqrt{d_1})$ in the first case or $K_n(\sqrt{-d_0})$ in the second case, and $K_n(\sqrt{d_1})$ is still a uniform way. □

Now we prove Theorem 3.3. It is an example of Theorem A.9, an explicit version of the Gross–Zagier formula proved by Yuan–Zhang–Zhang [33]. Recall that

$$P_\chi = \sum_{t\in\Phi} f_n(P_n)^t \chi(t).$$

The summation on Φ is not canonical, so the expression is not the exact case to apply the formula. However, by Proposition 3.2, $2z_n = 2f_n(P_n)$ is defined over H_n and thus

$$2P_\chi = \sum_{t\in\Phi} (2f_n(P_n))^t \chi(t) = \sum_{t\in \mathrm{Cl}_n} (2f_n(P_n))^t \chi(t).$$

This is the situation to apply the Gross–Zagier formula (to the test vector $2f_n$).

First, we see that the point P_χ is non-torsion only if χ satisfies the two conditions of Lemma 3.14. The first condition holds by considering the Tunnell–Saito theorem (cf. Theorem A.1). See the remarks after [33, Theorem 1.2] for example. For the second condition, assume that 2 is not split in $K = K_n$. By $\mathrm{Cl}_n = K^\times \backslash \widehat{K}^\times / \widehat{O}_K^\times$, the summation for $2P_\chi$ is essentially an integration on $K^\times \backslash \widehat{K}^\times$. By Proposition 3.1, f_n is invariant under the action of $K_2^\times$ up to torsions, so the integration is non-torsion only if χ is trivial on $K_2^\times$.

Hence, Lemma 3.14 implies the first statement of the theorem. Next, assume $\chi = \chi_{d_0,d_1}$ as in the theorem. Denote $P(d_0, d_1) = P_{\chi_{d_0,d_1}}$. We first have the following basic result.

LEMMA 3.15. *If* $(d_0, d_1) \equiv (5, 3) \pmod 8$*, then* $4P(d_0, d_1) \in A(\mathbb{Q}(\sqrt{d_0}))^- = [i]A(\mathbb{Q}(\sqrt{-d_0}))^-$*. Otherwise,* $4P(d_0, d_1) \in A(\mathbb{Q}(\sqrt{-d_0}))^-$*.*

Proof. Recall that

$$2P(d_0, d_1) = \sum_{t\in \mathrm{Cl}_n} (2z_n)^t \chi_{d_0,d_1}(t).$$

Then $2P(d_0, d_1)$ is invariant under the action of $\ker(\chi_{d_0,d_1}) = \mathrm{Gal}(H_n/K_{d_0,d_1})$. Then $2P(d_0, d_1)$ is defined over K_{d_0,d_1}. Here $K_{d_0,d_1} = K_n(\sqrt{-d_1})$ if $(d_0, d_1) \equiv (5, 3) \pmod 8$, and $K_{d_0,d_1} = K_n(\sqrt{d_1})$ otherwise.

First, assume that $d_1 \neq 1$, so that $[K_{d_0,d_1} : \mathbb{Q}] = 4$. Consider the action of $\mathrm{Gal}(K_{d_0,d_1}/\mathbb{Q})$ on $2P(d_0, d_1)$. The group $\mathrm{Gal}(K_{d_0,d_1}/\mathbb{Q})$ has two explicit elements: the complex conjugation c and the unique nontrivial element τ of $\mathrm{Gal}(K_{d_0,d_1}/K_n)$. By definition, χ takes -1 on any lifting of τ in Cl_n. It follows that

$$(2P(d_0, d_1))^\tau = -2P(d_0, d_1).$$

On the other hand, the complex conjugate

$$(2P(d_0, d_1))^c = \sum_{t\in \mathrm{Cl}_n} (2\bar{z}_n)^{1/t} = \sum_{t\in \mathrm{Cl}_n} (2\bar{z}_n)^t.$$

By Theorem 3.6, if $n \equiv 5, 6 \pmod 8$, then $2\bar{z}_n = -2z_n$. It follows that $(2P(d_0, d_1))^c = -2P(d_0, d_1)$. If $n \equiv 7 \pmod 8$, we only have $2\bar{z}_n = -2z_n^{\sigma_{\varpi^5}} + \tau(1)$, which gives

$$(2P(d_0, d_1))^c = -2\chi_{d_0,d_1}(\sigma_\varpi)P(d_0, d_1) + |\mathrm{Cl}_n|\tau(1).$$

Here

$$\chi_{d_0,d_1}(\sigma_\varpi) = -1 \iff \sigma_\varpi(\sqrt{d_1^*}) = -\sqrt{d_1^*} \iff (d_0, d_1) \equiv (5, 3) \pmod 8.$$

In summary, if $(d_0, d_1) \not\equiv (5, 3) \pmod 8$ (and $d_1 \neq 1$), then

$$(4P(d_0, d_1))^\tau = -4P(d_0, d_1), \quad (4P(d_0, d_1))^c = -4P(d_0, d_1).$$

It follows that $4P(d_0, d_1)$ is invariant under $c\tau$, and thus defined over

$$K^{c\tau}_{d_0,d_1} = \mathbb{Q}(\sqrt{-d_0}, \sqrt{d_1})^{c\tau} = \mathbb{Q}(\sqrt{-d_0}).$$

The action of τ further gives $4P(d_0, d_1) \in A(\mathbb{Q}(\sqrt{-d_0}))^-$. If $(d_0, d_1) \equiv (5, 3) \pmod 8$, then

$$(4P(d_0, d_1))^\tau = -4P(d_0, d_1), \quad (4P(d_0, d_1))^c = 4P(d_0, d_1).$$

It follows that $4P(d_0, d_1)$ is invariant under c, and thus defined over

$$K^c_{d_0,d_1} = \mathbb{Q}(\sqrt{d_0}, \sqrt{-d_1})^c = \mathbb{Q}(\sqrt{d_0}).$$

The action of τ further gives $4P(d_0, d_1) \in A(\mathbb{Q}(\sqrt{d_0}))^-$.

In the last case $d_1 = 1$, we have $K_{d_0,d_1} = K_n$. Then $(4P(d_0, d_1))^c = 4P(d_0, d_1)$ implies $4P(d_0, d_1) \in A(\mathbb{Q}(\sqrt{-d_0}))^-$. □

Go back to the proof of the theorem. Now we are ready to prove the formula

$$P_\chi = \epsilon(d_0, d_1)2^{h_2(n)}\mathcal{L}(d_1)\mathcal{P}(d_0) \ \in \ A(H'_n(i)) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

The formula is equivalent to

$$2\bar{\epsilon}(d_0, d_1)P_\chi = 2^{h_2(n)+1}\mathcal{L}(d_1)\mathcal{P}(d_0).$$

By Lemma 3.15, this is an identity in $A(K_{d_0})^- \otimes_{\mathbb{Z}} \mathbb{Q}$.

We first claim that the equality is true up to a multiple in $\mathbb{Q}^\times$. In fact, if $L'(A_{K_n}, \chi, 1) = L'(A_{d_0}, 1)L(A_{d_1}, 1)$ is zero, then the right-hand side is zero by definition, and P_χ is zero since the canonical height $\widehat{h}(P_\chi) = 0$ by the Gross–Zagier formula (in either [33, Theorem 1.2] or the explicit version Theorem A.9). If $L'(A_{K_n}, \chi, 1) \neq 0$, then by the theorems of Gross–Zagier and Kolyvagin, $E(K_{d_0})^- \otimes_{\mathbb{Z}} \mathbb{Q}$ is one-dimensional, and the thus two sides of the equality are proportional.

To finish the proof, it suffices to check that the two sides of the equality have the same canonical heights. One can do the whole computation on A, but we will carry it out on E to be compatible with our original framework.

Let $\varphi : A \to E$ be the isogeny of degree 2. The desired formula becomes

$$R_\chi = \epsilon(d_0, d_1) 2^{h_2(n)} \mathcal{L}(d_1) \mathcal{R}(d_0) \ \in \ E(H_n'(i)) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Here $R_\chi = \varphi(P_\chi)$ and $\mathcal{R}(d_0) = \varphi(\mathcal{P}(d_0))$. The vector $\mathcal{R}(d_0) \in E(K_{d_0})^- \otimes_{\mathbb{Z}} \mathbb{Q}$ has an independent description. If $\mathcal{L}(d_0) = 0$, then $\mathcal{R}(d_0) = 0$. If $\mathcal{L}(d_0) \neq 0$, then the theorems of Gross–Zagier and Kolyvagin imply that $E(K_{d_0})^-$ is of rank one. In this case, $\mathcal{R}(d_0) = 2^{-1} \mathcal{L}(d_0) \beta_{d_0} \in E(K_{d_0})^-_{\mathbb{Q}}$, where $\beta_{d_0} \in E(K_{d_0})^-$ is any $\mathbb{Z}$-basis of the free part of $E(K_{d_0})^-$.

The height identity we need to check is

$$\widehat{h}(R_\chi) = 4^{h_2(n)-1} \mathcal{L}(d_1)^2 \mathcal{L}(d_0)^2 \widehat{h}(\beta_{d_0}).$$

Assuming $L'(E_{K_n}, \chi, 1) \neq 0$. By the definitions of $\mathcal{L}(d_1)$ and $\mathcal{L}(d_0)$ in the introduction, the identity becomes

$$\widehat{h}(R_\chi) = L'(E_{K_n}, \chi, 1) / (2^{2k(n)-2h_2(n)-2-a(n)} \Omega_{d_0,\infty} \Omega_{d_1,\infty}).$$

Apply Theorem A.9, the explicit Gross-Zagier formula in the appendix, for $(E_{K_n}, \chi_{d_0,d_1})$ and the morphism $\varphi \circ f_n$. The proof is finished by computations similar to that in the proof of Theorem 2.1.

In the proof, we also see that $\mathcal{L}(n) \in \mathbb{Q}$. For example, the height formula

$$\widehat{h}(R_\chi) = 4^{h_2(n)-1} \mathcal{L}(d_1)^2 \mathcal{L}(d_0)^2 \widehat{h}(\beta_{d_0})$$

actually implies that $\mathcal{L}(d_1)\mathcal{L}(d_0) \in \mathbb{Q}$. Setting $d_1 = 1$, we see that $\mathcal{L}(n) \in \mathbb{Q}$.

Proof of Proposition 3.4. Here we prove Proposition 3.4 which asserts that

$$\begin{aligned} P(n) \equiv & \sum_{\substack{n = d_0 d_1 \cdots d_\ell \\ d_0 \equiv 5,6,7 \pmod 8 \\ d_1 \equiv 1,2,3 \pmod 8 \\ d_i \equiv 1 \pmod 8, \ i > 1}} \epsilon(d_0, d_1) \left(\prod_{i \geq 1} g(d_i) \right) Z(d_0) \\ & + i \sum_{\substack{n = d_0 d_1 \cdots d_\ell \\ (d_0, d_1, d_2) \equiv (5,3,2) \pmod 8 \\ d_i \equiv 1 \pmod 8, \ i > 2}} \left(\prod_{i \geq 1} g(d_i) \right) Z(d_0) \qquad \bmod \ 2A(\mathbb{H}_n'). \end{aligned}$$

It suffices to prove that the above formula (applied to every $P(d_0)$ below) and the formula in Theorem 1.1 (applied to every $\mathcal{L}(d_1)$ below) satisfies

$$Z(n) \equiv \sum_{\substack{n = d_0 d_1 \\ d_0 \equiv 5,6,7 \pmod 8 \\ d_1 \equiv 1,2,3 \pmod 8}} \epsilon(d_0, d_1) \mathcal{L}(d_1) P(d_0) \qquad \bmod \ 2A(\mathbb{H}_n').$$

We first treat the case $n \equiv 5, 7 \pmod 8$. Then the formula simplifies as

$$P(n) \qquad \equiv \qquad \sum_{\substack{n=d_0d_1\cdots d_\ell \\ d_0\equiv 5,7 \pmod 8 \\ d_1 \equiv 1,3 \pmod 8 \\ d_i\equiv 1 \pmod 8,\ i>1}} \epsilon(d_0,d_1)\left(\prod_{i\geq 1} g(d_i)\right) Z(d_0) \qquad \mathrm{mod} \qquad 2A(\mathbb{H}_n').$$

We need to check that

$$Z(n) \equiv \sum_{\substack{n=d_0d_1 \\ d_0\equiv 5,7 \pmod 8 \\ d_1\equiv 1,3 \pmod 8}} \epsilon(d_0,d_1)\left(\sum_{\substack{d_1=d_0'd_1'\cdots d_{\ell'}' \\ d_j'\equiv 1 \pmod 8,\ j>0}} \prod_{j\geq 0} g(d_j')\right)$$
$$\left(\sum_{\substack{d_0=d_0''d_1''\cdots d_{\ell''}'' \\ d_0''\equiv 5,7 \pmod 8 \\ d_1''\equiv 1,3 \pmod 8 \\ d_k''\equiv 1 \pmod 8,\ k>1}} \epsilon(d_0'',d_1'')\prod_{k\geq 1} g(d_k'')Z(d_0'')\right) \qquad \mathrm{mod}\ 2A(\mathbb{H}_n').$$

The right-hand side is a $\mathbb{Z}$-linear combination of

$$\epsilon(d_0,d_1)\epsilon(d_0'',d_1'')\prod_{j=0}^{\ell'} g(d_j')\prod_{k=1}^{\ell''} g(d_k'')Z(d_0'').$$

Consider the multiplicity of this term in the sum. Each appearance of such a terms gives a partition

$$\{d_1',\cdots,d_{\ell'}',d_2'',\cdots,d_{\ell''}''\} = \{d_1',\cdots,d_{\ell'}'\}\cup\{d_2'',\cdots,d_{\ell''}''\}.$$

If this set is non-empty, the number of such partitions is even, and thus the contribution is zero in the congruence equation. Moreover, if $d_0' \equiv 1 \pmod 8$ or $d_1'' \equiv 1 \pmod 8$, then we can also put it into the partition and deduce that the contribution of such terms is still zero.

Note that the contribution by $d_0 = d_0'' = n, d_1 = 1$ is the single term $Z(n)$. Therefore, it is reduced to check

$$0 \equiv \sum_{\substack{n=d_0d_1 \\ d_0\equiv 5,7 \pmod 8 \\ d_1\equiv 3 \pmod 8}} \epsilon(d_0,d_1)g(d_1) \sum_{\substack{d_0=d_0''d_1'' \\ d_0''\equiv 5,7 \pmod 8 \\ d_1''\equiv 3 \pmod 8}} \epsilon(d_0'',d_1'')g(d_1'')Z(d_0'') \qquad \mathrm{mod}\ 2A(\mathbb{H}_n').$$

Rewrite it as

$$0 \equiv \sum_{n=d_0''d_1''d_1}{}' \epsilon(d_0''d_1'',d_1)\epsilon(d_0'',d_1'')g(d_1)g(d_1'')Z(d_0'') \qquad \mathrm{mod}\ 2A(\mathbb{H}_n').$$

Here the sum is over ordered decompositions $n = d_0''d_1''d_1$ which satisfy the original congruence conditions (with $d_0 = d_0''d_1''$). The ordered decomposition $n = d_0''d_1''d_1$

corresponds to the ordered decomposition $n = d_0''d_1d_1''$ uniquely. One checks in this case

$$\epsilon(d_0''d_1'', d_1)\epsilon(d_0'', d_1'') = \pm\epsilon(d_0''d_1, d_1'')\epsilon(d_0'', d_1).$$

Then the sum is divisible by 2.

Now we treat the case $n \equiv 6 \pmod 8$. We need to check

$$Z(n) \equiv \sum_{\substack{n=d_0d_1\\ d_0\equiv 6,7 \pmod 8\\ d_1\equiv 1,2 \pmod 8}} \left(\sum_{\substack{d_1=d_0'd_1'\cdots d_{\ell'}'\\ d_j'\equiv 1 \pmod 8,\ j>0}} \prod_{j\geq 0} g(d_j') \right) \cdot$$

$$\left(\sum_{\substack{d_0=d_0''d_1''\cdots d_{\ell''}''\\ d_0''\equiv 5,6,7 \pmod 8\\ d_1''\equiv 1,2,3 \pmod 8\\ d_k''\equiv 1 \pmod 8,\ k>1}} \epsilon(d_0'', d_1'') \prod_{k\geq 1} g(d_k'')Z(d_0'') + i \sum_{\substack{d_0=d_0''d_1''\cdots d_{\ell''}''\\ (d_0'',d_1'',d_2'')\equiv(5,3,2) \pmod 8\\ d_k''\equiv 1 \pmod 8,\ k>2}} \prod_{k\geq 1} g(d_k'')Z(d_0'') \right)$$
$$\mod 2A(\mathbb{H}_n').$$

Split the outer sum $d = d_0d_1$ into the case $(d_0, d_1) \equiv (6, 1) \pmod 8$ and the case $(d_0, d_1) \equiv (7, 2) \pmod 8$. We obtain three triple sums, since the conditions $(d_0, d_1) \equiv (7, 2) \pmod 8$ and $(d_0'', d_1'', d_2'') \equiv (5, 3, 2) \pmod 8$ do not hold simultaneously. Similar to the case $n \equiv 5, 7 \pmod 8$, the contribution of the terms with some $d_j' \equiv 1 \pmod 8$ or some $d_k'' \equiv 1 \pmod 8$ is divisible by 2. In particular, for the case $d_1 \equiv 1 \pmod 8$, we are only left with $d_1 = 1$. Then it is reduced to check

$$0 \equiv \sum_{\substack{n=d_0d_1\\ d_0\equiv 7 \pmod 8\\ d_1\equiv 2 \pmod 8}} \left(g(d_1)Z(d_0) + \sum_{\substack{d_0=d_0''d_1''\\ d_0''\equiv 5 \pmod 8\\ d_1''\equiv 3 \pmod 8}} i\, g(d_1)g(d_1'')Z(d_0'') \right)$$
$$+ \sum_{\substack{n=d_0''d_1''\\ d_0''\equiv 7 \pmod 8\\ d_1''\equiv 2 \pmod 8}} g(d_1'')Z(d_0'') + i \sum_{\substack{n=d_0''d_1''d_2''\\ (d_0'',d_1'',d_2'')\equiv(5,3,2) \pmod 8}} g(d_1'')g(d_2'')Z(d_0'') \mod 2A(\mathbb{H}_n').$$

This is true by obvious cancellations, which finishes the proof of the proposition.

Torsion points. To prepare the proof of Theorem 3.5, we present some results on torsion points of A. They will be the key to lower multiples of algebraic points.

Denote $F = \mathbb{Q}(i)$. Recall that we have fixed an identification $A(\mathbb{C}) \cong \mathbb{C}/(1+i)O_F$, which gives $A(\mathbb{C})_{\mathrm{tor}} = A(F^{\mathrm{ab}})_{\mathrm{tor}} \cong F/(1+i)O_F$. Under the identification, the complex conjugation on $A(F^{\mathrm{ab}})_{\mathrm{tor}}$ is given by the conjugation $i \mapsto -i$ on F, The induced action of the Galois group $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ on $F/(1+i)O_F$ is given by multiplying by the composition

$$\mathrm{Gal}(F^{\mathrm{ab}}/F) \xrightarrow{\sigma_F^{-1}} F^\times\backslash\widehat{F}^\times \cong (1 + (1 + i)^3\widehat{O}_F)^\times.$$

Lemma 3.16. *Over F, the elliptic curve A_F is isomorphic to E_F. Moreover,*

$$\mathbb{Q}(A[4]) = \mathbb{Q}(\sqrt{2}, i), \quad A(\mathbb{Q}(i)) = A[(1+i)^3].$$

Proof. The results can be checked by explicit computations, but we include a theoretical proof. For the first statement, consider the two 2-isogenies

$$\varphi_F : A_F \longrightarrow E_F, \quad [1+i] : A_F \longrightarrow A_F.$$

One checks that these two morphisms have the same kernel $\{0, \tau(1)\}$. It follows that there is an isomorphism $A_F \to E_F$ carrying $[1+i]$ to ψ_F.

Now we treat $\mathbb{Q}(A[4])$. It is easy to have $F = \mathbb{Q}(A[2]) \subset \mathbb{Q}(A[4])$, and thus $\mathbb{Q}(A[4]) = F(A[4])$. The Galois action of $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ on $A[4]$ is given by

$$s_4 : (1 + (1+i)^3 \widehat{O}_F)^\times \longrightarrow (1 + (1+i)^3 O_{F_2})/(1 + 4O_{F_2}).$$

The field $F(A[4])$ is given by the subfield of F^{ab} fixed by $\ker(s_4) = (1 + 4\widehat{O}_F)^\times$, which is the ring class field of F of conductor 4. The norm map

$$(1 + (1+i)^3 O_{F_2})/(1 + 4O_{F_2}) \simeq (1 + 4\mathbb{Z}_2)/(1 + 8\mathbb{Z}_2)$$

implies that $F(A[4])$ is equal to the ring class field $\mathbb{Q}(\zeta_8)$ of $\mathbb{Q}$.

For $A(\mathbb{Q}(i))$, we first see that it is torsion since $A_1(\mathbb{Q}) \simeq A_{-1}(\mathbb{Q})$ are torsion. We also have $A(\mathbb{Q}(i))[p] = 0$ for any odd prime p. In fact, we can show that any nontrivial element of $A[p]$ has a residue field ramified above p and cannot be defined over $\mathbb{Q}(i)$. This argument will be used in Lemma 3.18 in a more complicated situation, so we omit it here.

Finally, we show that $A(\mathbb{Q}(i))[2^\infty] = A[(1+i)^3]$. Note that the stabilizer of any element x_4 of $A[4] \setminus A[(1+i)^3]$ is still $\ker(s_4)$. Then the residue field $F(x_4)$ is still $\mathbb{Q}(\zeta_8)$, and thus $x_4 \notin A(\mathbb{Q}(i))$. It follows that $A[4](\mathbb{Q}(i)) = A[(1+i)^3]$. □

Lemma 3.17. *Let $\kappa \in \mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ be the element sending ζ_8 to ζ_8^5. Then*

$$(\kappa+1)A[4] = A[4][\kappa+1] = A[2], \qquad (\kappa+1)E[4] = E[4][\kappa+1] = E[2].$$

Here $(\kappa+1)A[4]$ and $A[4][\kappa+1]$ are respectively the image and the kernel of the map

$$\kappa + 1 : A[4] \longrightarrow A[4], \quad x \longmapsto x^\kappa + x.$$

Proof. The results for A and E are equivalent since they are isomorphic over $F = \mathbb{Q}(i)$. Note that κ acts on $\mathbb{Q}(\zeta_8) \subset F^{\mathrm{ab}}$ as $\sigma_{F,2}(\pm 1 \pm 2i) = \sigma_{F,2}(\pm 2 \pm i)$. In terms of the CM theory, κ acts on $A[4] \cong O_F/4O_F$ by multiplication by $-1 \pm 2i \in 1 + (1+i)^3 O_{F_2}$. Then $\kappa + 1$ acts by multiplication by $\pm 2i$. The results are true. □

Lemma 3.18. *The torsion subgroup $A(\mathbb{H}'_n)_{\mathrm{tor}} = A[(1+i)^3]$ if n is odd, and $A(\mathbb{H}'_n)_{\mathrm{tor}} = A[4]$ if n is even.*

Proof. We prove the results by three steps.

Step 1. The group $A(\mathbb{H}'_n)[p] = 0$ for any odd prime p. Let $\wp$ be a prime ideal of F above p. The action of the Galois group on $A[\wp]$ gives a homomorphism

$$\mathrm{Gal}(F^{\mathrm{ab}}/F) \longrightarrow \mathrm{Aut}_{O_F}(A[\wp]) = (O_F/\wp)^\times.$$

This map is surjective since it is given by

$$s_\wp : (1 + (1+i)^3 \widehat{O}_F)^\times \longrightarrow O_{F_\wp}^\times \longrightarrow (O_F/\wp)^\times.$$

As a consequence, we have the following two properties:

(1) For any nonzero $x \in A[\wp]$, the residue field $F(x) = F(A[\wp])$ has degree $N(\wp) - 1 \geq 4$ over F.

(2) The prime $\wp$ is totally ramified in $F(x)$.

On the other hand, we claim that the ramification index of $\wp$ in $\mathbb{H}'_n$ is at most 2. In fact, $\mathbb{H}'_n$ is the composite of $L_n(i)$ and H'_{d_0} for different d_0, where the extensions $L_n(i)/K_n$ and H'_{d_0}/K_{d_0} do not involve ramification above p. If follows that we only need to consider the ramification index of p in the composite of K_n and K_{d_0} for different d_0, which is at most 2.

Combining the claim and the properties (1) and (2), we see that $F(x)$ cannot be contained in $\mathbb{H}'_n$. In other words, $A(\mathbb{H}'_n)[\wp] = 0$. Then $A(\mathbb{H}'_n)[p] = 0$. Hence, $A(\mathbb{H}'_n)_{\mathrm{tor}} = A(\mathbb{H}'_n)[2^\infty]$.

Step 2. For any $n \equiv 5, 6, 7 \pmod 8$, $A(\mathbb{H}'_n)[2^\infty] \subset A[4]$. Note that $A(\mathbb{H}'_n)[2^\infty]$ is a finite O_F-module, so it must be of the form $A[(1+i)^e]$ for some positive integer e. Thus it suffices to prove $|A(\mathbb{H}'_n)[2^\infty]| \leq 16$.

The idea is to use the reduction map to obtain the bound. Take a prime number $p \nmid (2n)$, and let v be a place of $\mathbb{H}'_n$ above p. Denote by $k(v)$ the residue field of v. The reduction map gives an injection

$$A(\mathbb{H}'_n)[2^\infty] \longrightarrow A(k(v))[2^\infty].$$

We will choose p carefully to get an easy bound on the right-hand side. In fact, we choose p satisfying the following properties:

(1) $p \equiv 3 \pmod 8$.

(2) p is inert in K_{d_0} for any positive factor d_0 of n with $d_0 \equiv 5, 6 \pmod 8$.

Assuming the existence of such p, we first see how it implies the desired bound. The proof consists of two steps. The first step is to show that $k(v) = \mathbb{F}_{p^2}$. Denote by w the restriction of v to $L_n(i)$, and v_{d_0} the restriction of v to H'_{d_0}. It is easy to see that the residue field $k(w) = \mathbb{F}_{p^2}$. To prove $k(v) = \mathbb{F}_{p^2}$, it suffices prove that $k(v_{d_0}) \subset \mathbb{F}_{p^2}$ for any $d_0 \equiv 5, 6 \pmod 8$. Note that p is inert in K_{d_0}. Then it suffices to check that $pO_{K_{d_0}}$ is totally split in H'_{d_0}. By Lemma 3.2, H'_{d_0} is contained in the ring class field $H_{d_0,4}$ of conductor 4. We claim that $pO_{K_{d_0}}$ is totally split in $H_{d_0,4}$. In fact, by the class field theory, it is equivalent to the easy fact that the image of p under the composition

$$K_{d_0,p}^\times \longrightarrow \widehat{K}_{d_0}^\times \longrightarrow K_{d_0}^\times \backslash \widehat{K}_{d_0}^\times / (\widehat{\mathbb{Z}} + 4\widehat{O}_{K_{d_0}})^\times = \mathrm{Gal}(H_{d_0,4}/K_{d_0})$$

is trivial.

The second step is to show that $|A(\mathbb{F}_{p^2})[2^\infty]| \leq 16$. This is done by explicit computation. In fact, by the choice $p \equiv 3 \pmod 8$, we see that A has supersingular reduction at p. Then the eigenvalues of the absolute Frobenius φ_p on the Tate modules of A are $\pm\sqrt{-p}$, so the eigenvalues of φ_p^2 are $-p, -p$. It follows that

$$|A(\mathbb{F}_{p^2})| = p^2 + 1 - (-p - p) = (p+1)^2.$$

By the choice $p \equiv 3 \pmod 8$, we have $|A(\mathbb{F}_{p^2})[2^\infty]| = 16$. This finishes the second step.

Finally, we check the existence of the prime p satisfying the two conditions. The second condition is equivalent to $(-d_0/p) = -1$, which becomes $(d_0/p) = 1$ by the first condition. Then we choose p satisfying:

(a) $p \equiv 3 \pmod 8$.

(b) $(\ell/p)=1$ for any prime factor ℓ of n with $\ell\equiv 1 \pmod 4$.

(c) $(\ell/p)=-1$ for any prime factor ℓ of n with $\ell\equiv -1 \pmod 4$.

It is easy to check that it gives $(d_0/p)=1$ for any $d_0\equiv 5,6 \pmod 8$. Now the existence of p satisfying (a), (b) and (c) is just a combination of the quadratic reciprocity law, the Chinese remainder theorem, and Dirichlet's density theorem.

Step 3. If n is odd, then $A(\mathbb{H}'_n)[2^\infty]=A[(1+i)^3]$. We will prove $\sqrt{2}\notin\mathbb{H}'_n$, which implies $A(\mathbb{H}'_n)_{\mathrm{tor}}=A[(1+i)^3]$ by Lemma 3.16.

To prove $\sqrt{2}\notin\mathbb{H}'_n$, note that $\mathbb{H}'_n$ is the composite of $L_n(i)$ and H'_{d_0} for some $d_0\equiv 5 \pmod 8$. Let v be a place of $\mathbb{H}'_n$ above 2, and v_{d_0} the restriction to H'_{d_0}. It suffices to show $\sqrt{2}\notin(\mathbb{H}'_n)_v$. Consider the ramification of v above 2. Note that $(\mathbb{H}'_n)_v$ is the composite of $\mathbb{Q}_2(i)$ and $(H'_{d_0})_{v_{d_0}}$ for all related d_0. By Proposition 3.2, $(H'_{d_0})_{v_{d_0}}$ is unramified over $N_{d_0,4}=(M_{d_0,4})^{\sigma_{1+2\varpi_{d_0}}}$, where $\varpi_{d_0}=(\sqrt{-d_0}-1)_2$ and $M_{d_0,4}$ is the ring class field of $\mathbb{Q}_2(\sqrt{-d_0})$ of conductor 4.

We claim that $N_{d_0,4}$ is independent of d_0. In fact, fix an isomorphism $\mathbb{Q}_2(\sqrt{-d_0})\cong\mathbb{Q}_2(\sqrt{-5})$, which induces an isomorphism $M_{d_0,4}\cong M_{5,4}$. Note that $1+2\varpi_{d_0}$ and $1+2\varpi_5$ have the same image in $K_{5,2}^\times/(\mathbb{Z}_2+4O_{K_{5,2}})^\times$, so their actions on $M_{5,4}$ are the same. It follows that $N_{d_0,4}=N_{5,4}$.

Note that $i\in N_{5,4}$ and $\sqrt{2}\notin N_{5,4}$. Therefore, $(\mathbb{H}'_n)_v$ is unramified over $N_{5,4}$. To prove $\sqrt{2}\notin(\mathbb{H}'_n)_v$, it suffices to prove that $N_{5,4}(\sqrt{2})=M_{5,4}$ is ramified over $N_{5,4}$. This is clear since $\mathrm{Gal}(M_{5,4}/N_{5,4})$ is generated by $\sigma_{1+2\varpi_5}$ with $1+2\varpi_5\in O_{K_{5,2}}^\times$. □

Proof of Theorem 3.5: representative. By definition, $\Phi_0\subset\Phi$. Recall that

$$P_\chi=\sum_{t\in\Phi}f_n(P_n)^t\chi(t).$$

Summing over all characters $\chi:\mathrm{Cl}_n\cong\mathrm{Cl}'_n/\langle\sigma\rangle\to\{\pm1\}$. We have

$$\sum_{\chi:\mathrm{Cl}_n\to\{\pm1\}}P_\chi=\sum_{t\in\Phi}f_n(P_n)^t\sum_{\chi:\mathrm{Cl}_n\to\{\pm1\}}\chi(t).$$

As in the case $n\equiv 1,2,3 \pmod 8$, apply the character formula

$$\sum_{\chi:\mathrm{Cl}_n\to\{\pm1\}}\chi(t)=2^{h_2(n)}\delta_{2\mathrm{Cl}_n}(t),\qquad t\in\mathrm{Cl}_n.$$

Here $h_2(n)=\dim_{\mathbb{F}_2}\mathrm{Cl}_n/2\mathrm{Cl}_n$. Then we obtain

$$\sum_{\chi:\mathrm{Cl}_n\to\{\pm1\}}P_\chi=2^{h_2(n)}\sum_{t\in\Phi_0}f_n(P_n)^t=2^{h_2(n)}Z(n).$$

This is an equality in $A(H'_n)$.

By Theorem 3.3, the equality gives

$$\sum_{\substack{n=d_0d_1\\ d_0\equiv 5,6,7 \pmod 8\\ d_1\equiv 1,2,3 \pmod 8,\ d_1>0}}\epsilon(d_0,d_1)2^{h_2(n)}\mathcal{L}(d_1)\mathcal{P}(d_0)=2^{h_2(n)}Z(n)\ \in\ A(H'_n(i))\otimes_{\mathbb{Z}}\mathbb{Q}.$$

We end up with

$$\sum_{\substack{n=d_0d_1\\ d_0\equiv 5,6,7 \pmod 8\\ d_1\equiv 1,2,3 \pmod 8,\ d_1>0}}\epsilon(d_0,d_1)\mathcal{L}(d_1)\mathcal{P}(d_0)=Z(n)\ \in\ A(H'_n(i))\otimes_{\mathbb{Z}}\mathbb{Q}.$$

Then we have

$$\mathcal{P}(n) = Z(n) - \sum_{\substack{n=d_0d_1 \\ d_0\equiv 5,6,7 \pmod 8 \\ d_1\equiv 1,2,3 \pmod 8,\ d_1>1}} \epsilon(d_0,d_1)\mathcal{L}(d_1)\mathcal{P}(d_0).$$

It follows that $\mathcal{P}(n)$ and $P(n)$ satisfy the same iteration formula (in different groups). Therefore, $P(n)$ represents $\mathcal{P}(n)$. This proves the first statement of the theorem.

Proof of Theorem 3.5: part (1). Here we prove part (1) of the theorem. Let $R(n)$ (resp. $R(d_0,d_1)$) be the image of $P(n)$ (resp. $P(d_0,d_1) = P_{\chi_{d_0,d_1}}$) under the 2-isogeny from A to E. Then $R(n) \in E(\mathbb{H}'_n)$ and $R(d_0,d_1) \in E(H'_n)$. We need to prove that $2R(n) \in E(K_n)^-$.

Note that in Lemma 3.15 we have already checked $4P(n,1) \in A(K_n)^-$ and thus $4R(n,1) \in E(K_n)^-$. To relate to $2R(n)$, we have the following simple connection.

Lemma 3.19.

$$4P(n,1) = \pm 2^{2+h_2(n)}P(n), \qquad 4R(n,1) = \pm 2^{2+h_2(n)}R(n).$$

Proof. By Theorem 3.3,

$$P(n,1) = \pm 2^{h_2(n)}P(n) \ \in\ A(\mathbb{H}'_n)\otimes_{\mathbb{Z}}\mathbb{Q}.$$

Then

$$P(n,1) \mp 2^{h_2(n)}P(n) \ \in\ A(\mathbb{H}'_n)_{\mathrm{tor}} = A(\mathbb{H}'_n)[4].$$

Here the last identity follows from Lemma 3.18. □

Before proving part (1) of the theorem, we introduce some notations on fields. Recall that H_n is the Hilbert class field of $K_n = \mathbb{Q}(\sqrt{-n})$ and $H'_n = H_n(f_n(P_n))$. Recall that $K'_n = K_n, K_n(i), K_n$ for $n \equiv 5,6,7 \pmod 8$ respectively. Let $L_n \subset H_n$ be the genus field of K_n; that is, L_n is subfield of H_n fixed by the subgroup $2\mathrm{Cl}_n$ of $\mathrm{Cl}_n = \mathrm{Gal}(H_n/K_n)$. Define $L'_n = L_n, L_n(i), L_n$ for $n \equiv 5,6,7 \pmod 8$ respectively. Then $L'_n = L_nK'_n$. Set $K''_n = K_n(E[4](L'_n))$, i.e. $K''_n = K_n(i), K_n(\sqrt{2},i), K_n$ for $n \equiv 5,6,7 \pmod 8$ respectively.

First, we prove $2R(n) \in E(K''_n)$. Consider the image of $4R(n,1) = \pm 2^{h_2(n)+2}R(n)$ under the (injective) Kummer map

$$\delta : E(K''_n)/2^{h_2(n)+2}E(K''_n) \longrightarrow H^1(K''_n, E[2^{h_2(n)+2}]),$$

and the inflation-restriction exact sequence

$$1 \longrightarrow \mathrm{Hom}(\mathrm{Gal}(L'_n/K''_n), E[4](K''_n)) \longrightarrow H^1(K''_n, E[2^{h_2(n)+2}]) \longrightarrow H^1(L'_n, E[2^{h_2(n)+2}]).$$

(Note that $E[2^\infty](L'_n) = E[4](K''_n)$.) The image of $\delta(2^{h_2(n)+2}R(n))$ in $H^1(L'_n, E[2^{h_2(n)+2}])$ is 0, since it is 0 in $E(L'_n)/2^{h_2(n)+2}E(L'_n)$. Then $\delta(2^{h_2(n)+2}R(n))$ lies in $\mathrm{Hom}(\mathrm{Gal}(L'_n/K''_n), E[4](K''_n))$, which has exponent 2 since $\mathrm{Gal}(L'_n/K''_n)$ has exponent 2. It follows that $\delta(2^{h_2(n)+3}R(n)) = 0$. Thus

$$2^{h_2(n)+3}R(n) \in 2^{h_2(n)+2}E(K''_n), \qquad 2R(n) \in E(K''_n) + E[2^\infty](L'_n) = E(K''_n).$$

Second, we prove $2R(n) \in E(K_n)^-$ for $n \equiv 7 \pmod 8$. This is the simplest case, but it illustrates the key idea. In this case, we already have $2R(n) \in E(K_n)$, and we need to prove $2\overline{R(n)} = -2R(n)$. By Lemma 3.15 and Lemma 3.19,

$$2^{h_2(n)+2}(R(n) + \overline{R(n)}) = \pm(4R(n,1) + 4\overline{R(n,1)}) = 0.$$

Then $R(n) + \overline{R(n)} \in E(K_n)[2^\infty] = E[2]$ is killed by 2. The result follows.

Third, we prove $2R(n) \in E(K_n)^-$ for $n \equiv 5 \pmod 8$. It suffices to prove $2R(n) \in E(K_n)$, since the process from $E(K_n)$ to $E(K_n)^-$ is the same as the case $n \equiv 7 \pmod 8$. We already know $2R(n) \in E(K_n(i))$. Denote by $\xi \in \mathrm{Gal}(K_n(i)/K_n)$ the unique non-trivial element, and take a lifting of ξ to $\mathrm{Gal}(\mathbb{H}'_n/K_n)$, which we still denote by ξ. By Lemma 3.15 and Lemma 3.19,

$$2^{h_2(n)+2}(P(n)^\xi - P(n)) = \pm(4P(n,1)^\xi - 4P(n,1)) = 0.$$

Then $P(n)^\xi - P(n) \in A(K_n(i))[2^\infty] = A[(1+i)^3]$. Note that $A[(1+i)^3]$ is exactly killed by $2\varphi : A \to E$. We have $2R(n)^\xi - 2R(n) = 0$, and thus $2R(n) \in E(K_n)$.

For the case $n \equiv 6 \pmod 8$, we need the following simple result.

Lemma 3.20. *For any $n \equiv 5, 6, 7 \pmod 8$, $R(n) \in E(L_n(i))$.*

Proof. By the recursion formula, it suffices to prove $\varphi(Z(n)) \in E(L'_n)$ for any $n \equiv 5, 6, 7 \pmod 8$. By Theorem 3.6, $\varphi(z_n)$ is invariant under the action of σ. Here σ is described right after Proposition 3.2. If $n \equiv 5, 7 \pmod 8$, then $\varphi(z_n)$ is defined over H_n, and thus $\varphi(Z(n))$ is defined over L_n. If $n \equiv 6 \pmod 8$, then $\varphi(z_n)$ is defined over $H_n(i)$, and thus $\varphi(Z(n))$ is defined over $L_n(i)$. □

Finally, we prove $2R(n) \in E(K_n)^-$ for $n \equiv 6 \pmod 8$. We already know $2R(n) \in E(K_n(\sqrt{2}, i))$. It suffices to prove $2R(n) \in E(K_n(i))$, since the process from $E(K_n(i))$ to $E(K_n)^-$ is the same as that for the case $n \equiv 5 \pmod 8$.

Let $\kappa \in \mathrm{Gal}(K_n(\sqrt{2}, i)/K_n(i))$ be the unique non-trivial element, and take any lifting of κ in $\mathrm{Gal}(L_n(i)/K_n(i))$, still denoted by κ. We need to show that $(2R(n))^\kappa = 2R(n)$. Note that $\kappa^2 = 1$ since $\mathrm{Gal}(L_n(i)/K_n(i))$ has exponent 2. By Lemma 3.15 and Lemma 3.19,

$$2^{h_2(n)+2}(R(n)^\kappa - R(n)) = \pm(4R(n,1)^\kappa - 4R(n,1)) = 0,$$

so $R(n)^\kappa - R(n)$ lies in $E[4][\kappa+1] = \{x \in E[4] : x^\kappa + x = 0\}$. By Lemma 3.17, $E[4][\kappa+1] = E[2]$. It follows that $2(R(n)^\kappa - R(n)) = 0$. The proof of part (1) is complete.

Proof of Theorem 3.5: part (2). We start with some Galois-theoretic preparation. Denote by

$$r : \mathbb{Q}^\times \backslash \mathbb{A}^\times \longrightarrow \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$$

the Artin map over $\mathbb{Q}$. Then $c = r_\infty(-1)$ is the complex conjugation. Define $\beta_1, \beta_2 \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ by

$$\beta_1 = r_\infty(-1)r_2(-2), \qquad \beta_2 = r_\infty(-1)r_2(6).$$

Let $\beta'_1, \beta'_2 \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be any liftings of β_1, β_2.

In the following, we take the convention that $(\gamma+1)R$ means $\gamma(R)+1$ for any $\gamma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The key of the proof is the following lemma.

Lemma 3.21.

(1) *For any* $n \equiv 5 \pmod 8$,

$$Z(n)^{\beta_1'+1} = Z(n)^{\beta_2'+1} \ \in\ g(n)\ \tau(\frac{1-i}{2}) + \mathbb{Z}\,\tau(1).$$

(2) *For any* $n \equiv -2 \pmod{16}$,

$$Z(n)^{\beta_1'+1} \ \in\ g(n)\ \tau(\frac{i}{2}) + \mathbb{Z}\,\tau(1).$$

(3) *For any* $n \equiv 6 \pmod{16}$,

$$Z(n)^{\beta_2'+1} \ \in\ g(n)\ \tau(\frac{i}{2}) + \mathbb{Z}\,\tau(1).$$

(4) *For any* $n \equiv 7 \pmod 8$,

$$Z(n)^{\beta_1'+1} = Z(n)^{\beta_2'+1} = g(n)\ \tau(\frac{1}{2}).$$

Proof. Recall that after Proposition 3.2 we have introduced $\sigma \in 2\mathrm{Cl}_n'$ which gives

$$\mathrm{Cl}_n'/\langle\sigma\rangle \cong \mathrm{Cl}_n, \quad (2\mathrm{Cl}_n')/\langle\sigma\rangle \cong 2\mathrm{Cl}_n.$$

Note that the genus field L_n is the subfield of H_n fixed by $2\mathrm{Cl}_n$. It follows that the subfield of H_n' fixed by $2\mathrm{Cl}_n'$ is $L_n, L_n(i), L_n$ according to $n \equiv 5, 6, 7 \pmod 8$.

The field $L_n(i) = \mathbb{Q}(i, \sqrt{d} : d|n)$ is a subfield of $\mathbb{Q}^{\mathrm{ab}}$. It is easy to check that the action of the involved β_j' on $L_n(i)$ is the same as that of $\sigma_\varpi \circ c$ in all the four cases of the lemma. For example, if $n \equiv 5 \pmod 8$, then σ_ϖ acts on $L_n(i)$ as $r_2(N_{K_n/\mathbb{Q}}(\varpi)) = r_2(n+1) = r_2(-2)$. As a consequence, we claim that

$$Z(n)^{\beta_j'} - Z(n)^{\sigma_\varpi \circ c} \in \mathbb{Z}\,\tau(1)$$

in all four cases.

In fact, denote $\alpha = \sigma_\varpi \circ c \circ \beta_j'^{-1}$, viewed as an element of $\mathrm{Cl}_n' = \mathrm{Gal}(H_n'/K_n')$. It suffices to show

$$Z(n)^\alpha - Z(n) \in \mathbb{Z}\,\tau(1).$$

Since α acts trivially on $L_n(i)$, we see that $\alpha \in 2\mathrm{Cl}_n'$. Recall the definition

$$Z(n) = \sum_{t\in\Phi_0} z_n^t, \qquad Z(n)^\alpha = \sum_{t\in\alpha\Phi_0} z_n^t.$$

Here Φ_0 is a set of representatives of $2\mathrm{Cl}_n = (2\mathrm{Cl}_n')/\langle\sigma\rangle$ in $2\mathrm{Cl}_n'$. Then $\alpha\Phi_0$ is also a set of representatives of $2\mathrm{Cl}_n$ in $2\mathrm{Cl}_n'$. Write $\Phi_0 = \{t_i : i = 1, \cdots, g(n)\}$. Then $\alpha\Phi_0 = \{\sigma_i t_i : i = 1, \cdots, g(n)\}$, where each $\sigma_i \in \langle\sigma\rangle$. By Theorem 3.6, we see that $z_n^\sigma = z_n$ or $z_n^\sigma = z_n + \tau(1)$. It follows that

$$Z(n)^\alpha - Z(n) = \sum_{t_i\in\Phi_0} (z_n^{\sigma_i} - z_n)^{t_i} \in \mathbb{Z}\,\tau(1).$$

Therefore, the result for $Z(n)^{\beta_j'+1}$ becomes that for $Z(n)^{\sigma_\varpi\circ c+1}$, which can be checked easily by Theorem 3.6 for $n \equiv 5, 6 \pmod 8$. In the case $n \equiv 7 \pmod 8$, $H_n' = H_n$ and thus $Z(n)$ is already defined over L_n. Then

$$Z(n)^{\beta_j'} = Z(n)^{\sigma_\varpi \circ c} = Z(n)^{\sigma_{\varpi^5} \circ c}.$$

Here the last identity holds since the Galois group $\mathrm{Gal}(L_n(i)/\mathbb{Q})$ has exponent 2. Then the result for $Z(n)^{\beta'_j+1}$ still follows from Theorem 3.6. □

Now we prove part (2) of Theorem 3.5. Assume that $P(n) = P + t$ for some $P \in A(K_n)^-$ and $t \in A[4]$. Define $\beta \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ by

$$\beta = \begin{cases} r_\infty(-1)r_2(-2) & \text{if } n \equiv 5, 7 \pmod 8 \text{ or } n \equiv -2 \pmod{16}, \\ r_\infty(-1)r_2(6) & \text{if } n \equiv 6 \pmod{16}. \end{cases}$$

Let $\beta' \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be any liftings of β. Explicit calculation shows that β acts on K_n by $\sqrt{-n} \mapsto -\sqrt{-n}$. It follows that $P(n)^\beta + P(n) = t^\beta + t$.

We first treat the case $n \equiv 5, 7 \pmod 8$. Then $t \in A(\mathbb{H}'_n)[4] = A(\mathbb{Q}(i))$ by Lemma 3.18. Note that β acts on $\mathbb{Q}(i)$ trivially. Then $P(n)^\beta + P(n) = 2t \in \mathbb{Z}\tau(1)$. Apply $\beta' + 1$ to both sides of Proposition 3.4. By Lemma 3.21, we have

$$\left(i^{\frac{n-1}{2}} \sum_{\substack{n=d_0 d_1 \cdots d_\ell \\ d_0 \equiv 5 \pmod 8 \\ d_1 \equiv 1,3 \pmod 8 \\ d_i \equiv 1 \pmod 8,\ i>1}} \prod_i g(d_i) \right) \tau\left(\frac{1-i}{2}\right) + \left(\sum_{\substack{n=d_0 d_1 \cdots d_\ell \\ d_0 \equiv 7 \pmod 8 \\ d_1 \equiv 1,3 \pmod 8 \\ d_i \equiv 1 \pmod 8,\ i>1}} \prod_i g(d_i) \right) \tau\left(\frac{1}{2}\right) \in 2A(\mathbb{H}'_n)^{\beta'+1} + \mathbb{Z}\tau(1).$$

It follows that the contribution from $2A(\mathbb{H}'_n)^{\beta'+1}$ is torsion, which is contained in

$$2A(\mathbb{H}'_n)_{\mathrm{tor}} = 2A(\mathbb{Q}(i)) = \mathbb{Z}\,\tau(1).$$

Then the left-hand side lies in $\mathbb{Z}\,\tau(1)$. Thus the coefficients in both of the brackets must be even.

Now we treat the case $n \equiv 6 \pmod 8$. In this case we can only have the weaker result

$$P(n)^\beta + P(n) \in (\beta + 1)A[4] = A[2]$$

by Lemma 3.17. Apply $\beta'+1$ to Proposition 3.4 again. We get

$$\left(\sum_{\substack{n=d_0d_1\cdots d_\ell\\ d_0\equiv 6\,(\mathrm{mod}\,8)\\ d_i\equiv 1\,(\mathrm{mod}\,8),\ i>0}} \prod_i g(d_i)\right)\tau(\frac{i}{2}) + \left(\sum_{\substack{n=d_0d_1\cdots d_\ell\\ d_0\equiv 7\,(\mathrm{mod}\,8)\\ d_1\equiv 2\,(\mathrm{mod}\,8)\\ d_i\equiv 1\,(\mathrm{mod}\,8),\ i>1}} \prod_i g(d_i)\right)\tau(\frac{1}{2})$$

$$+ \left(i\sum_{\substack{n=d_0d_1\cdots d_\ell\\ (d_0,d_1,d_2)\equiv(5,3,2)\,(\mathrm{mod}\,8)\\ d_i\equiv 1\,(\mathrm{mod}\,8),\ i>2}} \prod_{i\geq 1} g(d_i)\right)\tau(\frac{1-i}{2}) \ \in\ 2A(\mathbb{H}'_n)^{\beta'+1}+A[2].$$

The contribution of $2A(\mathbb{H}'_n)^{\beta'+1}$ is a torsion point, and thus lies in $2A[4]=A[2]$. Then the left-hand side lies in $A[2]$. It follows that the first two coefficients have the same parity, which is the same as the assertion of the theorem in this case. This finishes the proof of Theorem 3.5.

Appendix A. Explicit Formulae. In this appendix, we prove an explicit Waldspurger formula and an explicit Gross–Zagier formula in the case that the character χ on the quadratic extension is unramified. The results are derived from the original Waldspurger formula (cf. [33, Theorem 1.4]) and the Yuan–Zhang–Zhang version of the Gross–Zagier formula proved in [33, Theorem 1.2].

All global L-functions in this section are complete L-functions with archimedean components normalized to have center $s=1/2$. To avoid confusion, we use $L(s,1_F)$ to denote the complete Dedekind zeta functions of a number field F, which is the product of the usual Dedekind zeta function $\zeta_F(s)$ with the gamma factors.

A.1. Theorem of multiplicity one. As in [33, Chapter 1], the Waldspurger formula and the Gross–Zagier formula can be interpreted as identities of certain one-dimensional spaces of functionals. In this section, we briefly recall the local results about this space of functionals.

Let F be a local field and B a quaternion algebra over F. Then B is isomorphic to either $M_2(F)$ or the unique division quaternion algebra over F. The Hasse invariant $\epsilon(B)=1$ if $B\simeq M_2(F)$, and $\epsilon(B)=-1$ if B is the division algebra.

Let K be either $F\oplus F$ or a quadratic field extension over F, with a fixed embedding $K\hookrightarrow B$ of algebras over F. Let $\eta: F^\times\to\mathbb{C}^\times$ be the (quadratic or trivial) character associated to the extension K/F.

Let π be an irreducible admissible representation of $B^\times$ with central character ω_π, and let $\chi: K^\times\to\mathbb{C}^\times$ be a character of $K^\times$ such that

$$\omega_\pi\cdot\chi|_{F^\times}=1.$$

Define the co-invariant space

$$(\pi\otimes\chi)_{K^\times}:=\{\ell\in\mathrm{Hom}_{\mathbb{C}}(\pi,\mathbb{C}):\ell(\pi(t)v)=\chi^{-1}(t)\ell(v),\ \forall\ v\in\pi,\ t\in K^\times\}.$$

The following result asserts that the dimension of this space is determined by the local root number of the Rankin–Selberg L-function $L(\frac{1}{2},\pi,\chi)$.

Theorem A.1 (Tunnell [28], Saito [24]). *The dimension* $\dim\,(\pi\otimes\chi)_{K^\times}\leq 1$, *and the equality holds if and only if*

$$\epsilon(B)=\chi(-1)\eta(-1)\epsilon(\frac{1}{2},\pi,\chi).$$

We also consider the invariant subspace

$$(\pi\otimes\chi)^{K^\times}=\{v\in\pi:\pi(t)v=\chi^{-1}(t)v,\ \forall\, t\in K^\times\}.$$

Corollary A.2. *One has*

$$\dim\,(\pi\otimes\chi)^{K^\times}\leq\dim\,(\pi\otimes\chi)_{K^\times}.$$

If K is a field, then the equality holds.

Proof. Denote by $\pi^\vee$ the contragredient of π. The natural inclusion $\pi\hookrightarrow\mathrm{Hom}_{\mathbb{C}}(\pi^\vee,\mathbb{C})$ induces an injection

$$(\pi\otimes\chi)^{K^\times}\longrightarrow(\pi^\vee\otimes\chi^{-1})_{K^\times}.$$

It follows that

$$\dim\,(\pi\otimes\chi)^{K^\times}\leq\dim\,(\pi^\vee\otimes\chi^{-1})_{K^\times}=\dim\,(\pi\otimes\chi)_{K^\times}.$$

Here the last equality follows from the theorem since $\epsilon(\frac{1}{2},\pi^\vee,\chi^{-1})=\epsilon(\frac{1}{2},\pi,\chi)$. This proves the first assertion.

For the second assertion, assuming $\dim\,(\pi\otimes\chi)_{K^\times}=1$, we need to construct a nonzero element of $(\pi\otimes\chi)^{K^\times}$. Take $\ell\in(\pi\otimes\chi)_{K^\times}$ and $v\in\pi$ such that $\ell(v)\neq 0$. Since K is a field, the quotient $K^\times/F^\times$ is compact. Fix a Haar measure on $K^\times/F^\times$. Then

$$w=\int_{K^\times/F^\times}\chi(t)\pi(t)vdt$$

is an element of π. Furthermore,

$$\ell(w)=\int_{K^\times/F^\times}\chi(t)\ell(\pi(t)v)dt=\int_{K^\times/F^\times}\ell(v)dt=\mathrm{vol}(K^\times/F^\times)\ \ell(v)\neq 0.$$

It follows that $w\neq 0$, which finishes the proof. □

A.2. Explicit Waldspurger formula. Let F be a number field and $\mathbb{A}$ its ring of adeles. Let B be a quaternion algebra over F and G the algebraic group $B^\times$ over F. Denote by $Z\cong F^\times$ the center of G. Let π be a unitary cuspidal automorphic representation of $G(\mathbb{A})$ and ω_π its central character. Let K be a quadratic field extension over F, T the algebraic group $K^\times$ over F, η its associated quadratic Hecke character on $\mathbb{A}^\times$. Let $\chi:K^\times\backslash\mathbb{A}_K^\times\to\mathbb{C}^\times$ be a Hecke character of finite order. Assume that

- $\omega_\pi\cdot\chi|_{\mathbb{A}^\times}=1$.
- For each place v of F, $\epsilon(1/2,\pi_v,\chi_v)\cdot\eta_v(-1)\chi_v(-1)=\mathrm{inv}(B_v)$.

It follows that the global root number $\epsilon(1/2, \pi, \chi)$ of $L(s, \pi, \chi)$ is $+1$ and there is an F-embedding $K \subset B$, which we fix once for all and via which T is viewed as a sub-torus of G. By Theorem A.1, the space

$$(\pi \otimes \chi)_T := \{\ell \in \mathrm{Hom}_{\mathbb{C}}(\pi, \mathbb{C}) : \ell(\pi(t)f) = \chi^{-1}(t)\ell(f), \ \forall\ f \in \pi,\ t \in T(\mathbb{A})\}$$

is one-dimensional.

Let $P_\chi : \pi \to \mathbb{C}$ be the period functional defined by

$$P_\chi(f) = \int_{T(F)Z(\mathbb{A})\backslash T(\mathbb{A})} f(t)\chi(t)dt, \quad \forall f \in \pi.$$

Here the Haar measure is normalized by $\mathrm{vol}(Z(\mathbb{A})T(F)\backslash T(\mathbb{A}), dt) = 2L(1, \eta)$. Note that P_χ is a natural element of $(\pi \otimes \chi)_T$. The Waldspurger formula tells when it is non-zero.

Theorem A.3 (Waldspurger formula, [33], Theorem 1.4). *For any non-zero pure tensor $f = \otimes_v f_v \in \pi$,*

$$\frac{|P_\chi(f)|^2}{(f, f)_{\mathrm{Pet}}} = \frac{1}{2} \frac{L(1/2, \pi, \chi)}{L(1, \pi, \mathrm{ad})L(2, 1_F)^{-1}} \cdot \beta(f).$$

The notations are explained as follows:

(1) *$\beta(f) = \prod_v \beta_v(f_v)$ is a product over all places v of F and for each v,*

$$\beta_v(f_v) := \frac{L(1, \eta_v)L(1, \pi_v, \mathrm{ad})}{L(2, 1_v)L(1/2, \pi_v, \chi_v)} \int_{Z(F_v)\backslash T(F_v)} \frac{(\pi_v(t_v)f_v, f_v)_v}{(f_v, f_v)_v} \chi_v(t_v)dt_v,$$

where $(\ ,\ )_v$ is any non-trivial $B_v^\times$-invariant Hermitian pairing on π_v. The Haar measures are normalized by $\otimes_v dt_v = dt$ and $\mathrm{vol}(Z(\mathbb{A})T(F)\backslash T(\mathbb{A}), dt) = 2L(1, \eta)$.

(2) *$(f, f)_{\mathrm{Pet}}$ is the Peterson norm of $f \in \pi$ defined by*

$$(f, f)_{\mathrm{Pet}} = \int_{G(F)Z(\mathbb{A})\backslash G(\mathbb{A})} |f(g)|^2 dg,$$

where the Haar measure dg is the Tamagawa measure such that the volume of $G(F)Z(\mathbb{A})\backslash G(\mathbb{A})$ is 2.

The goal of this subsection is to give an explicit form of Waldspurger's formula under the following assumptions:

(a) F is totally real and K is quadratic and totally imaginary over F;
(b) χ_v is unramified for each place $v \nmid \infty$;
(c) for any $v|\infty$, the Jacquet-Langlands correspondence π_v^{JL} is a discrete series of weight k_v on $\mathrm{GL}_2(\mathbb{R})$ with $k_v \geq 2$ even integer.

It follows that the central character ω_π of π is unramified everywhere.

Let O_F be the ring of integers in F and O_v be the ring of integers in F_v for any finite place v of F. For any $a \in \mathbb{A}^\times$, let $|a|$ denote its adelic absolute valuation such that $dax = |a|dx$ for any Haar measure dx on $\mathbb{A}^\times$. We view $F_v^\times$ and the finite part $\mathbb{A}_f^\times$ of F as subrings of $\mathbb{A}^\times$.

Let $N, D, d \in \mathbb{A}_f^\times$ be such that for any finite place v of F, N_v generates the conductor of π_v^{JL} of π, D_v generates the relative discriminant of K_v/F_v, and d_v generates the different of F_v. For each $v \nmid \infty$, let R_v be an order of $B_v := B \otimes_F F_v$ with discriminant $N_v O_v$ such that $R_v \cap K_v = O_{K_v}$. Such an order exists and is unique up to conjugacy of $K_v^\times$. Recall that a Gross-Prasad test vector $f \in \pi$ for the pair π and χ is a pure tensor $f = \otimes_v f_v$ defined as follows (see [8]).

(1) If v is finite with $\mathrm{ord}_v(N_v) \leq 1$ or K_v/F_v is unramified, then $\pi_v^{R_v^\times}$ is of dimension one and $f_v \in \pi_v^{R_v^\times}$ is a non-zero vector.

(2) If v is finite with $\mathrm{ord}_v(N_v) \geq 2$ and K_v/F_v is ramified, then the space

$$(\pi_v \otimes \chi_v)^{K_v^\times} = \{f_v \in \pi_v : \pi_v(t) f_v = \chi_v^{-1}(t) f_v,\ \forall\, t \in K_v^\times\}$$

is one-dimensional by Theorem A.2. The vector f_v is any non-zero element in this space.

(3) If v is real, let f_v be any non-zero element of the one-dimensional space $(\pi_v \otimes \chi_v)^{K_v^\times}$.

Thus a Gross-Prasad test vector for (π, χ) is unique up to scalar.

Let π^{JL} be the Jacquet-Langlands correspondence of π on $\mathrm{GL}_2(\mathbb{A})$. The Hilbert newform $f' \in \pi^{\mathrm{JL}}$ is the unique form of level $U_1(N)$ such that $\mathrm{SO}_2(\mathbb{R}) \subset \mathrm{GL}_2(F_v)$ acts by the character $\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \mapsto e^{2\pi i k_v \theta}$ for each $v|\infty$, and such that

$$L(s, \pi^{\mathrm{JL}}) = 2^{[F:\mathbb{Q}]} \cdot |d|^{s-\frac{1}{2}} \cdot \int_{F^\times \backslash \mathbb{A}^\times} f'\begin{pmatrix} a & \\ & 1 \end{pmatrix} |a|^{s-\frac{1}{2}} d^\times a,$$

where the measure $d^\times a$ is chosen such that

$$\mathrm{Res}_{s=1} \int_{|a|\leq 1, a \in F^\times \backslash \mathbb{A}^\times} |a|^{s-1} d^\times a = \mathrm{Res}_{s=1} L(s, 1_F).$$

Theorem A.4 (Explicit Waldspurger Formula). *Assume the conditions (a), (b) and (c). Let f' be the newform of π^{JL} and f a Gross-Prasad test vector. Then*

$$\begin{aligned}
&\frac{1}{(f,f)_{\mathrm{Pet}}} \cdot \Big| \sum_{t \in \widehat{K}^\times / K^\times \widehat{F}^\times \widehat{O}_K^\times} f(t)\chi(t) \Big|^2 \\
&= \kappa^2 \cdot [O_K^\times : O_F^\times]^2 \cdot 2^{[F:\mathbb{Q}]} \cdot \frac{L^{((N,D)\infty)}(1/2, \pi, \chi)}{(f', f')_{\mathrm{Pet}} |Dd^2|^{1/2}} \cdot \prod_{v|\infty} (4\pi)^{-(k_v+1)} \Gamma(k_v) \\
&\quad \cdot \prod_{v|N \text{ inert}} (1 - q_v^{-1})(1 + q_v^{-1})^{-1} \cdot \prod_{v||N \text{ ramified}} 2(1 + q_v^{-1})^{-1} \cdot \prod_{v^2|N \text{ ramified}} 2(1 - q_v^{-1}),
\end{aligned}$$

where $\kappa = 1$ or 2 is the order of the kernel of the natural morphism from the ideal class group of F to that of K, and (N, D) is the set of places v such that both $\mathrm{ord}_v(N)$ *and* $\mathrm{ord}_v(D)$ *are positive.*

Here as before, $(f', f')_{\mathrm{Pet}}$ and $(f, f)_{\mathrm{Pet}}$ denote the Peterson norms with respect to the Tamagawa measures on $Z\backslash\mathrm{GL}_2$ and $Z\backslash G$ respectively. To deduce the explicit formula, we first calculate the local factors.

Proposition A.5. *Let (π, χ, f) as above. Let e_v be the ramification index of E_v over F_v. Then we have*

$$|Dd|_v^{-1/2}\ \beta(f_v) = \begin{cases} e_v(1-q_v^{-e_v})\dfrac{L(1,\pi_v,\mathrm{ad})}{L(1/2,\pi_v,\chi_v)}, & \textit{if } v|N \textit{ non-split,} \\ \dfrac{L(1,1_v)}{L(2,1_v)}, & \textit{if } v||N \textit{ split,} \\ \dfrac{L(1,1_v)L(1,\pi_v,\mathrm{ad})}{L(2,1_v)}, & \textit{if } v^2|N \textit{ split,} \\ 1, & \textit{otherwise.} \end{cases}$$

Remark A.6. For each place $v \nmid \infty$, note that the central character ω_v of π_v is unramified and then $\omega_v = \mu_v^2$ for some unramified character μ. So we may assume that π_v is of trivial central character. Let $\iota_i, i = 1, 2$ be two embeddings of K_v in $B(F_v)$ then they are conjugate by an element $\gamma \in G(F_v)$. Let R_1 be the order above and f_1 a test vector, then $\gamma R_1 \gamma^{-1}$ is an order and $f_2 = \pi_v(\gamma)(f_1)$ is a test vector under ι_2. We have that $\beta_v(f_1) = \beta_v(f_2)$.

Proof. We are in the local situation, omitting the subscript v, let K denote the quadratic extension of local field F. Denote $n = \mathrm{ord}_v(N)$. Reduce to compute the toric integral

$$\beta^0 = \int_{F^\times\backslash K^\times} \frac{\langle \pi(t)f, f\rangle}{\langle f, f\rangle}\chi(t)dt.$$

If $n > 0$ and K is nonsplit, then f is χ^{-1}-eigen and $\beta^0 = \mathrm{vol}(F^\times\backslash K^\times)$. For the other cases, the order R in the definition of $V(\pi, \chi)$ is an Eichler order of discriminant n. We fix the following embedding of K so that $R = R_0(n) := \begin{pmatrix} O & O \\ \mathfrak{p}^n & O \end{pmatrix}$ and we can take the test vector as the new vector W_0. If $K = F^2$ is split, embed K into $M_2(F)$ by $(a, b) \longmapsto \begin{pmatrix} a & \\ & b \end{pmatrix}$. If K is a field, take $\tau \in O_K$ such that $O_K = O[\tau]$ and such that if K/F is ramified then τ is a uniformizer. Let $\mathrm{Tr}\tau, \mathrm{N}\tau \in F$ denote the trace and norm of τ, respectively. Embed K into B by

$$a + b\tau \longmapsto \begin{pmatrix} a + b\mathrm{Tr}\tau & b\mathrm{N}\tau \\ -b & a \end{pmatrix}.$$

Assume $K = F^2$. We write $K^\times = F^\times K^1$ with the image of K^1 in $\mathrm{GL}_2(F)$ equal to $\begin{pmatrix} * & \\ & 1 \end{pmatrix}$. Denote by χ_1 the restriction of χ to K^1, then

$$\begin{aligned} \beta^0 &= (W_0, W_0)^{-1} \iint_{(F^\times)^2} W_0\left[\begin{pmatrix} ab & \\ & 1 \end{pmatrix}\right] \overline{W_0\left[\begin{pmatrix} b & \\ & 1 \end{pmatrix}\right]} \chi_1(a) d^\times b d^\times a \\ &= (W_0, W_0)^{-1} |Z(1/2, W_0, \chi_1)|^2. \end{aligned}$$

Now $Z(1/2, W_0, \chi_1) = \chi_1(d)^{-1}L(1/2, \pi \otimes \chi_1)$ and

$$\beta^0 = (W_0, W_0)^{-1}L(1/2, \pi, \chi).$$

Now consider the case that K is a field and π is unramified. Let

$$\Psi(g) := \frac{(\pi(g)W_0, W_0)}{(W_0, W_0)}, \qquad g \in \mathrm{GL}_2(F).$$

Then

$$\beta^0 = \frac{\mathrm{vol}(K^\times/F^\times)}{\# K^\times/F^\times O_K^\times} \sum_{t \in K^\times/F^\times O_K^\times} \Psi(t)\chi(t).$$

If K/F is unramified, then

$$\beta^0 = \mathrm{vol}(K^\times/F^\times) = |d|^{1/2}$$

while if K/F is ramified,

$$\beta^0 = |Dd|^{1/2}(1 + \Psi(\tau)\chi(\tau)).$$

Using MacDonald formula for the matrix coefficient $\Psi(\tau)$, we obtain

$$\beta(f) = |Dd|^{1/2}.$$

□

Proof of Theorem A.4. The proof is just a calculation of the right-hand side of the formula in Theorem A.3. Apply the expression of $\beta(f_v)$ in Proposition A.5. We also need the a special value formula for $L(1, \pi, \mathrm{ad})$, which will be proved in Theorem

A.10 in the next subsection. Then the formula gives

$$\begin{aligned}
&\frac{\left||Dd|^{-1/2}P_\chi(f)\right|^2}{(f,f)_{\mathrm{Pet}}}\\
=&\frac{L^{(\infty)}(1/2,\pi,\chi)}{(f',f')_{\mathrm{Pet}}|Dd^2|^{1/2}}\left(\frac{2}{\pi}\right)^{[F:\mathbb{Q}]}(4\pi)^{-\sum_v k_v}\prod_v\Gamma(k_v)\\
&\qquad\cdot\frac{\prod_{v\nmid\infty}\beta_v(f_v)|Dd|_v^{-1/2}}{L_N(1,\pi,\mathrm{ad})\prod_{v|N}(1+q_v^{-1})\prod_{v\|N}(1-q_v^{-2})}\\
=&\frac{L^{(\infty)}(1/2,\pi,\chi)}{(f',f')_{\mathrm{Pet}}|Dd^2|^{1/2}}\prod_{v|\infty}\left(2^{1-2k_v}\pi^{-(k_v+1)}\Gamma(k_v)\right)\\
&\cdot\prod_{v||N}\frac{\beta_v(f_v)|Dd|_v^{-1/2}}{(1+q_v^{-1})}\cdot\prod_{v^2|N}\frac{\beta_v(f_v)|Dd|_v^{-1/2}}{L_v(1,\pi_v,\mathrm{ad})(1+q_v^{-1})}\cdot\prod_{v\nmid N\infty}\beta_v(f_v)|Dd|_v^{-1/2}\\
=&\frac{L^{(\infty)}(1/2,\pi,\chi)}{(f',f')_{\mathrm{Pet}}|Dd^2|^{1/2}}\prod_{v|\infty}\left(2^{1-2k_v}\pi^{-(k_v+1)}\Gamma(k_v)\right)\cdot\prod_{v|c}\beta_v(f_v)|Dd|_v^{-1/2}\\
&\cdot\prod_{v||N\ \mathrm{nonsplit}}\frac{\beta_v(f_v)|Dd|_v^{-1/2}}{(1+q_v^{-1})}\cdot\prod_{v^2|N\ \mathrm{nonsplit}}\frac{\beta_v(f_v)|Dd|_v^{-1/2}}{L_v(1,\pi_v,\mathrm{ad})(1+q_v^{-1})},\\
=&\frac{L^{(\infty)}(1/2,\pi,\chi)}{(f',f')_{\mathrm{Pet}}|Dd^2|^{1/2}}\prod_{v|\infty}\left(2^{1-2k_v}\pi^{-(k_v+1)}\Gamma(k_v)\right)\\
&\cdot\prod_{v|N\ \mathrm{inert}}(1-q_v^{-1})(1+q_v^{-1})^{-1}\cdot\prod_{v||N\ \mathrm{ramified}}(1+q_v^{-1})^{-1}\cdot\prod_{v^2|N\ \mathrm{ramified}}(1-q_v^{-1})\\
&\cdot\prod_{v|N\ \mathrm{ramified}}2L(1/2,\pi_v,\chi_v)^{-1}.
\end{aligned}$$

It follows that

$$\begin{aligned}
\frac{\left||Dd|^{-1/2}P_\chi(f)\right|^2}{(f,f)_{\mathrm{Pet}}}=&\frac{L^{((N,D)\infty)}(1/2,\pi,\chi)}{(f',f')_{\mathrm{Pet}}|Dd^2|^{1/2}}\left(\prod_{v|\infty}2^{1-2k_v}\pi^{-(k_v+1)}\Gamma(k_v)\right)\\
&\cdot\prod_{v|N\ \mathrm{inert}}(1-q_v^{-1})(1+q_v^{-1})^{-1}\cdot\prod_{v||N\ \mathrm{ramified}}2(1+q_v^{-1})^{-1}\cdot\prod_{v^2|N\ \mathrm{ramified}}2(1-q_v^{-1}).
\end{aligned}$$

To finish the proof, we need the following simple result.

Lemma A.7. *Let F be a totally real field, K a totally imaginary quadratic extension over F, and η the associated quadratic character of $\mathbb{A}^\times$. Then*

$$\frac{2L(1,\eta)|Dd|^{-1/2}}{\#(\widehat{K}^\times/K^\times\widehat{F}^\times\widehat{O}_K^\times)}=\kappa^{-1}\cdot[O_K^\times:O_F^\times]^{-1}\cdot 2^{[F:\mathbb{Q}]}.$$

Here $\kappa=1$ or 2 is the cardinality of the kernel of natural morphism from the ideal class group of F to that of K.

Proof. It follows from the exact sequence

$$1\to(\widehat{F}^\times\cap K^\times\widehat{O}_K^\times)/F^\times\widehat{O}_F^\times\to\widehat{F}^\times/F^\times\widehat{O}_F^\times\to\widehat{K}^\times/K^\times\widehat{O}_K^\times\to\widehat{K}^\times/K^\times\widehat{F}^\times\widehat{O}_K^\times\to 1,$$

that

$$\#\widehat{K}^\times/K^\times\widehat{F}^\times\widehat{O}_K^\times = \frac{h_K}{h_F}\cdot\kappa,$$

where we use the fact that $\widehat{K}^\times/K^\times\widehat{O}_K^\times$ is isomorphic to the ideal class group of K and similarly for F. By the ideal class number formula:

$$L(1,\eta)|Dd|^{-1/2} = L(0,\eta) = \frac{h_K}{h_F}\cdot[O_K^\times : O_F^\times]^{-1}\cdot 2^{[F:\mathbb{Q}]-1}.$$

Thus we have that

$$\frac{L(1,\eta)|Dd|^{-1/2}}{\#\widehat{K}^\times/K^\times\widehat{F}^\times\widehat{O}_K^\times} = \kappa^{-1}\cdot[O_K^\times : O_F^\times]^{-1}\cdot 2^{[F:\mathbb{Q}]-1}.$$

□

Go back to proof of Theorem A.4. Note that

$$P_\chi(f) = \frac{2L(1,\eta)}{\#\widehat{K}^\times/K^\times\widehat{F}^\times\widehat{O}_K^\times}\sum_{t\in\widehat{K}^\times/K^\times\widehat{F}^\times\widehat{O}_K^\times} f(t)\chi(t).$$

We have that

$$|Dd|^{-1/2}P_\chi(f) = 2^{[F:\mathbb{Q}]}\kappa^{-1}[O_K^\times : O_F^\times]^{-1}\sum_{t\in\widehat{K}^\times/K^\times\widehat{F}^\times\widehat{O}_K^\times} f(t)\chi(t).$$

Thus we obtain the desired explicit formula in Theorem A.4. □

A.3. Explicit Gross-Zagier formula. We first recall the main theorem of [33]. Let F be a totally real number field and $\mathbb{A}$ its ring of adeles. Let X be the Shimura curve over F associated to an incoherent quaternion algebra $\mathbb{B}$ over $\mathbb{A}$ with ramification set Σ (containing all infinite places). Let ξ be the Hodge bundle on X, and let J be its Jacobian. Let A be a simple abelian variety defined over F parameterized by X. Then

$$\pi_A := \mathrm{Hom}^0_\xi(X,A) = \mathrm{Hom}^0(J,A),$$

is a representation of $\mathbb{B}^\times$ over $\mathbb{Q}$ whose infinite components are all trivial. It is known that $M := \mathrm{End}_{\mathbb{B}^\times}(\pi_A) = \mathrm{End}^0(A)$ is a number field of degree $\dim A$ over $\mathbb{Q}$. Let $(\ ,\ ) : \pi_A\times\pi_{A^\vee}\to M$ be the perfect $\mathbb{B}^\times$-pairing given by $(f_1,f_2) = \mathrm{vol}(X_U)^{-1}(f_{1,U}\circ f_{2,U}^\vee)$, where the composition uses the canonical isomorphism $J_U^\vee\cong J_U$ and the volume using the measure $dxdy/(2\pi y^2)$ on $\mathcal{H}$. Let

$$\langle\ ,\ \rangle_M :\ A(\bar{F})_{\mathbb{Q}}\otimes_M A^\vee(\bar{F})_{\mathbb{Q}}\longrightarrow M\otimes_{\mathbb{Q}}\mathbb{R}$$

be the M-bilinear height pairing whose trace to $\mathbb{R}$ is the usual height pairing.

Let K be a totally imaginary quadratic extension of F with a fixed embedding $K_{\mathbb{A}}\hookrightarrow\mathbb{B}$ over $\mathbb{A}$. Let $\chi:\widehat{K}^\times/K^\times\to L^\times$ be a Hecke character of finite order valued in a number field $L\supset M$, and also viewed as a Galois character via the class field theory. Assume that

- $\omega_{\pi_A}\cdot\chi|_{\mathbb{A}^\times} = 1$.
- $\epsilon(1/2,\pi_v,\chi_v)\cdot\chi_v\eta_v(-1) = \mathrm{inv}(\mathbb{B}_v)$ for each place v of F.

Then the global root number is -1. By Theorem A.1, these conditions imply that $(\pi_A \otimes \chi)_{K_{\mathbb{A}}^\times}$ is one-dimensional.

Denote

$$A(\chi) = (A(K^{\mathrm{ab}})_{\mathbb{Q}} \otimes_M L)^{\mathrm{Gal}(K^{\mathrm{ab}}/K)}.$$

Let $h_0 \in \mathcal{H}$ be the unique fixed point of $K^\times$. It defines a point $P = ([h_0, 1]_U)_U \in X$. Define the period map $P_\chi : \pi \to A(\chi)$ by

$$P_\chi(f) = \int_{t \in \widehat{K}^\times / K^\times \widehat{F}^\times} f(P)^{\sigma_t} \otimes_M \chi(t) dt,$$

where we use the Haar measure such that the volume of $\widehat{K}^\times / K^\times \widehat{F}^\times$ is $2L(1, \eta)$. The Gross-Zagier formula of Yuan-Zhang-Zhang is as follows.

Theorem A.8 (Yuan-Zhang-Zhang [33]). *For any pure tensors $f_1 \in \pi_A$ and $f_2 \in \pi_{A^\vee}$ with $(f_1, f_2) \neq 0$,*

$$\frac{\langle P_\chi(f_1), P_{\chi-1}(f_2)\rangle_L}{(f_1, f_2)} = \frac{L'(1/2, \pi_A, \chi)}{L(1, \pi_A, \mathrm{ad}) L(2, 1_F)^{-1}} \cdot \beta(f_1 \otimes f_2)$$

as an identity in $L \otimes_{\mathbb{Q}} \mathbb{C}$. Here $\langle \ , \ \rangle_L : A(\chi) \times A(\chi^{-1}) \to L \otimes_{\mathbb{Q}} \mathbb{R}$ is the L-linear Néron–Tate height pairing induced by the M-linear Néron–Tate height pairing $\langle \cdot, \cdot \rangle_M$ above.

Note that we can define Gross-Prasad test vectors as in the last subsection. Then the explicit version of the formula is as follows.

Theorem A.9 (Explicit Formula of Gross-Zagier). *Assume that χ is an unramified character of finite order. Let $f \in \pi_A$ be a Gross-Prasad test vector. Then*

$$\begin{aligned} &\frac{1}{(f, f)} \cdot \widehat{h}\left(\sum_{t \in \widehat{K}^\times / \widehat{F}^\times K^\times \widehat{O}_K^\times} f(P)^t \chi(t) \right) \\ &= \kappa^2 \cdot [O_K^\times : O_F^\times]^2 \cdot 2^{[F:\mathbb{Q}]+1} \cdot \frac{L'^{((N,D)\infty)}(1/2, \pi, \chi)}{(f', f')_{\mathrm{Pet}} |Dd^2|^{1/2} (4\pi)^{3[F:\mathbb{Q}]}} \\ &\cdot \prod_{v | N \text{ inert}} (1 - q_v^{-1})(1 + q_v^{-1})^{-1} \cdot \prod_{v || N \text{ ramified}} 2(1 + q_v^{-1})^{-1} \cdot \prod_{v^2 | N \text{ ramified}} 2(1 - q_v^{-1}). \end{aligned}$$

Here $\kappa = 1$ or 2 is the order of the morphism from the ideal class group of F to that of K, and (N, D) denotes the set of finite places v of F such that both $\mathrm{ord}_v(N)$ *and* $\mathrm{ord}_v(D)$ *are positive.*

The deduction of the theorem is almost the same as that of Theorem A.4, so we omit it here. One can obtain the original Gross–Zagier formula under the Heegner hypothesis from the above formula.

A.4. Special value formula of adjoint L-function. In the proof of Theorem A.4 and Theorem A.9, we have used the following formula.

Theorem A.10. *Let F be a totally real field and d_F the absolute discriminant of F. Let σ be a unitary cuspidal automorphic representation of* $\mathrm{GL}_2(\mathbb{A})$, *$N \subset O_F$ its* *conductor, and f the newform in σ. Assume that σ_v is discrete series of weight k_v for every $v|\infty$. Then*

$$\frac{L^{S'}(1,\sigma,\mathrm{ad})}{|d_F|^{1/2}\cdot(f,f)_{\mathrm{Pet}}\cdot L(2,1_F)}=2^{[F:\mathbb{Q}]-1+\sum_{v|\infty}k_v}\prod_{v|N}(1+q_v^{-1}),$$

where S' is the set of finite places v of F with conductor $n(\sigma_v)\geq 2$. Equivalently,

$$\frac{L^{(N\infty)}(1,\sigma,\mathrm{ad})}{|d_F|^{1/2}\cdot(f,f)_{\mathrm{Pet}}\cdot\zeta_F(2)}=\frac{(4\pi)^{\sum_v k_v}}{2\prod_v\Gamma(k_v)}\cdot\prod_{v|N}(1+q_v^{-1})\prod_{v\|N}(1-q_v^{-2}).$$

This formula can be found in the literature (probably under slightly different assumptions). We sketch a proof here for the readers. Set $G=\mathrm{GL}_2$ over F. Let N the unipotent subgroup of G consisting of matrices $\begin{pmatrix}1&a\\&1\end{pmatrix}$ in G, and $U=\prod_v U_v$ be a maximal compact subgroup of $G(\mathbb{A})$. We follow [33, §1.6] to normalize the non-trivial additive character $\psi:F\backslash\mathbb{A}\to\mathbb{C}^\times$ and Haar measures on $\mathbb{A}$, $\mathbb{A}^\times$ and $G(\mathbb{A})$ and their local components.

The proof of Theorem A.10 starts with the residue of an Eisenstein series. For any $\Phi\in\mathcal{S}(\mathbb{A}^2)$, define the Eisenstein series

$$E(s,g,\Phi):=\sum_{\gamma\in P(F)\backslash G(F)}P(s,\gamma g,\Phi),$$

where

$$P(s,g,\Phi)=|\det g|^s\int_{\mathbb{A}^\times}\Phi([0,b]g)|b|^{2s}d^\times b.$$

Lemma A.11. *The Eisenstein series $E(s,g,\Phi)$ has meromorphic continuation to the whole s-plane with only possible poles at $s=1,0$. In particular, if let $\widehat{\Phi}$ denote the Fourier transformation of Φ then*

$$\mathrm{Res}_{s=1}E(s,g,\Phi)=\frac{1}{2}\widehat{\Phi}(0)\cdot\mathrm{Res}_{s=1}L(s,1_F).$$

Proof. By the Poisson summation formula,

$$\begin{aligned}E(s,g,\Phi)&=|\det g|^s\int_{F^\times\backslash\mathbb{A}^\times}\left(\sum_{\xi\in F^2\backslash\{0\}}\Phi(a\xi g)\right)|a|^{2s}d^\times a\\&=|\det g|^s\int_{|a|\geq 1}\left(\sum_{\xi\in F^2\backslash\{0\}}\Phi(a\xi g)\right)|a|^{2s}d^\times a\\&\quad+|\det g|^{s-1}\int_{|a|\geq 1}\left(\sum_{\xi\in F^2\backslash\{0\}}\widehat{\Phi}(g^{-1}\xi^t a)\right)|a|^{2-2s}d^\times a\\&\quad+|\det g|^{s-1}\widehat{\Phi}(0)\int_{|a|\leq 1}|a|^{2s-2}d^\times a\\&\quad-|\det g|^s\Phi(0)\int_{|a|\leq 1}|a|^{2s}d^\times a.\end{aligned}$$

Thus $E(s,g,\Phi)$ has meromorphic continuation. Furthermore,

$$\mathrm{Res}_{s=1}E(s,g,\Phi)=\widehat{\Phi}(0)\cdot\lim_{s\to 1}(s-1)\int_{|a|\le 1}|a|^{2s-2}d^{\times}a=\frac{1}{2}\widehat{\Phi}(0)\cdot\mathrm{Res}_{s=1}L(s,1_F).$$

□

Let σ be as in Theorem A.10. Take any $f_1,f_2\in\sigma$. Let $W_1,W_2\in\mathcal{W}(\sigma,\psi)$ be the Whittaker functions associated to them. Namely, for $i=1,2$,

$$W_i(g)=\int_{N(F)\backslash N(\mathbb{A})}f_i(ng)\overline{\psi(n)}dn,$$

where the Haar measure on $N(\mathbb{A})$ is the one on $\mathbb{A}$ via the isomorphism $N(\mathbb{A})\cong\mathbb{A}$. As in [12], consider the integral

$$Z(s,f_1,f_2,\Phi):=\int_{G(F)\backslash G(\mathbb{A})/Z(\mathbb{A})}f_1(g)\overline{f_2(g)}E(s,g,\Phi)dg.$$

By unfolding the Eisenstein series, we obtain

$$Z(s,f_1,f_2,\Phi)=\int_{N(\mathbb{A})\backslash G(\mathbb{A})}|\det g|^sW_1(g)\overline{W_2(g)}\Phi([0,1]g)dg.$$

It is a product of local factors. The theorem will be obtained as the residue at $s=1$ of this expression.

For each place v of F and $\Phi_v\in\mathcal{S}(F_v^2)$, denote the local factor

$$Z(s,W_{1,v},W_{2,v},\Phi_v):=\int_{N(F_v)\backslash G(F_v)}|\det g|^sW_{1,v}(g)\overline{W_{2,v}(g)}\Phi_v([0,1]g)dg,$$

which has meromorphic continuation to the whole s-plane. Moreover, for any $v\nmid\infty$, the fractional ideal of $\mathbb{C}[q_v^s,q_v^{-s}]$ generated by all $Z(s,W_{1,v},W_{2,v},\Phi_v)$ with $W_{i,v}\in\mathcal{W}(\sigma_v,\psi_v)$ and $\Phi_v\in\mathcal{S}(F_v^2)$ is the same as that generated by $L(s,\sigma_v\times\widetilde{\sigma}_v)$.

To take the residue, we need to compute $Z(1,W_{1,v},W_{2,v},\Phi_v)$. The following result asserts that it is essentially the inner product on $\mathcal{W}(\sigma_v,\psi_v)$ given by

$$\langle W_{1,v},W_{2,v}\rangle=\int_{F_v^{\times}}W_{1,v}\begin{pmatrix}a&\\&1\end{pmatrix}\overline{W_{2,v}\begin{pmatrix}a&\\&1\end{pmatrix}}d^{\times}a.$$

Lemma A.12. *For each v,*

$$Z(1,W_{1,v},W_{2,v},\Phi_v)=\widehat{\Phi}_v(0)\cdot\langle W_{1,v},W_{2,v}\rangle.$$

Proof. This is a result of [12]. For any place v of F, let $d'k$ be the Haar measure on U_v determined by the following measure identity on $G(F_v)$:

$$dg=|b|dxd^{\times}ad^{\times}bd'k,\qquad g=a\begin{pmatrix}1&x\\&1\end{pmatrix}\begin{pmatrix}1&\\&b\end{pmatrix}k\in G(F_v).$$

By [12, p. 51],

$$Z(1,W_{1,v},W_{2,v},\Phi_v)=\int_{F_v^{\times}}W_{1,v}\begin{pmatrix}a&\\&1\end{pmatrix}\overline{W_{2,v}\begin{pmatrix}a&\\&1\end{pmatrix}}d^{\times}a\cdot\iint_{F_v^{\times}\times U_v}\Phi_v([0,b]k)|b|^2d^{\times}bd'k.$$

By [12, Lemma 2.3],

$$\iint_{F_v^\times \times U_v} \Phi([0,b]k)|b|^2 d^\times b dk = \widehat{\Phi}_v(0).$$

The result follows. □

Now we are ready to finish the proof of Theorem A.10. Let $\Phi = \otimes_v \Phi_v \in \mathcal{S}(\mathbb{A}^2)$ be any element with $\widehat{\Phi}(0) \neq 0$, and let f_1, f_2 be pure tensors. Take the residues at $s = 1$ on the two sides of

$$Z(s, f_1, f_2, \Phi) = \prod_v Z(s, W_{1,v}, W_{2,v}, \Phi_v).$$

Applying Lemmas A.12, we have

$$(f_1, f_2)_{\mathrm{Pet}} \cdot \mathrm{Res}_{s=1} E(s, g, \Phi) = \widehat{\Phi}(0) \cdot \mathrm{Res}_{s=1} L(s, \sigma \times \widetilde{\sigma}) \cdot \prod_v \frac{\langle W_{1,v}, W_{2,v} \rangle}{L(1, \sigma_v \times \widetilde{\sigma}_v)}.$$

We will see that the product on the right-hand side converges absolutely. Applying Lemma A.11, we have

$$\frac{L(1, \sigma, \mathrm{ad})}{(f_1, f_2)_{\mathrm{Pet}}} = \frac{1}{2} \prod_v \frac{L(1, \sigma_v \times \widetilde{\sigma}_v)}{\langle W_{1,v}, W_{2,v} \rangle}.$$

Let $f_1 = f_2 = f$ be the newform and $W^\circ = \otimes_v W_v^\circ$ the corresponding new vector. Then

$$\frac{L(1, \sigma, \mathrm{ad})}{(f, f)_{\mathrm{Pet}}} = \frac{1}{2} \prod_v \frac{L(1, \sigma_v \times \widetilde{\sigma}_v)}{\langle W_v^\circ, W_v^\circ \rangle}.$$

The proof is complete by the following result on the local factor.

Lemma A.13.

$$\frac{L(1, \sigma_v \times \widetilde{\sigma}_v) L(2, 1_{F_v})^{-1} |d_v|^{1/2}}{\langle W_v^\circ, W_v^\circ \rangle} = \begin{cases} 1, & n(\sigma_v) = 0, v \nmid \infty, \\ 1 + q_v^{-1}, & n(\sigma_v) = 1, v \nmid \infty, \\ (1 + q_v^{-1}) L(1, \sigma_v, \mathrm{ad}), & n(\sigma_v) \geq 2, v \nmid \infty, \\ 2^{k_v + 1}, & v | \infty. \end{cases}$$

Proof. The result follows directly from the explicit form of the Kirillov model for the new vector. Note that the new vector W_v° for $v|\infty$ is equal to

$$W_v^\circ(g) = |y|^{k/2} e^{2\pi i(x+iy)} e^{ik\theta} 1_{\mathbb{R}_+^\times}(\det g),$$

where $g = a \begin{pmatrix} y & x \\ & 1 \end{pmatrix} k_\theta \in \mathrm{GL}_2(\mathbb{R})$, which matches with $\frac{1}{2} L(s, \sigma_\infty)$ so that the corresponding Hilbert form is the (normalized) newform. □

REFERENCES

[1] B. J. Birch and N. M. Stephens, *The parity of the rank of the Mordell-Weil group*, Topology, 5 (1966), pp. 295–299.

[2] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc., 14 (2001), pp. 843–939.

[3] J. Coates, Y. Kezuka, Y. Li, and Y. Tian, *Iwasawa theory for the Gross family of elliptic curves with complex multiplication*, to appear.

[4] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math., 39 (1977), pp. 233–251.

[5] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, in Number theory, Carbondale 1979, M. B. Nathanson, ed., Lecture Notes in Math. 751, Springer, Berlin, 1979, pp. 108–118.

[6] C. Gonzalez-Aviles, *On the conjecture of Birch and Swinnerton-Dyer*, Trans. Amer. Math. Soc., 349 (1997), pp. 4181–4200.

[7] B. Gross, *Local Orders, Root Numbers, and Modular Curves*, American Journal of Mathematics, 110 (1988), pp. 1153–1182.

[8] B. Gross and D. Prasad, *Test vectors for linear forms*, Math. Ann., 291, (1991), pp. 343–355.

[9] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math., 84:2 (1986), pp. 225–320.

[10] K. Heegner, *Diophantische analysis und modulfunktionen*, Math. Z., 56 (1952), pp. 227–253.

[11] D. R. Heath-Brown, *The size of Selmer group for the congruent number problem, II*, Invent. math., 118 (1994), pp. 331–370.

[12] H. Jacquet and C. Nan, *Positivity of quadratic base change L-functions*, Bull Soc. math. France, 129:1 (2001), pp. 33–90.

[13] B. W. Jones and G. Pall, *Regular and semi-regular positive ternary quadratic forms*, Acta Mathematica, 70 (1939), pp. 165–191.

[14] N. M. Katz and P. Sarnak, *Zeros of zeta functions and symmetry*, Bull. Amer. Math. Soc. (N.S.), 36:1 (1999), pp. 1–26.

[15] S. Kobayshi, *The p-adic Gross-Zagier formula for elliptic curves at supersingular primes*, Invent. Math., 191:3 (2013), pp. 527–629.

[16] V. A. Kolyvagain, *Euler system*, The Grothendieck Festschrift. Prog. in ath., Boston, Birkhauser (1990).

[17] V. A. Kolyvagain, *Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil curves*, Math. USSR Izvestiya, 32:3 (1989).

[18] P. Monsky, *Mock Heegner Points and Congruent Numbers*, Math. Z., 204 (1990), pp. 45–68.

[19] P. Monsky, Appendix to D. R. Heath-Brown, *The size of Selmer group for the congruent number problem, II*, Invent. math., 118 (1994), pp. 331–370.

[20] B. Perrin-Riou, *Points de Heegner et dérivées de fonctions L p-adiques*, Invent. Math., 89:3 (1987), pp. 455–510.

[21] L. Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math., 171 (1934), pp. 55–60.

[22] K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math., 89:3 (1987), pp. 527–559.

[23] K. Rubin, *The"main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math., 103:1 (1991), pp. 25–68.

[24] H. Saito, *On Tunnell's formula for characters of* GL(2), Compositio Math., 85:1 (1993), pp. 99–108.

[25] A. Smith, *An approach to the full BSD conjecture at two in quadratic twist families of elliptic curves*, undergraduate thesis at Princeton.

[26] Y. Tian, *Congruent Numbers and Heegner Points*, Cambridge J. of Math, 2:1 (2014), pp. 117–161.

[27] Y. Tian, *Congruent numbers with many prime factors*, PNAS, 109:52, 21256-21258.

[28] J. Tunnell, *Local ϵ-factors and characters of* GL(2), Amer. J. Math., 105:6 (1983), pp. 1277–1307.

[29] J. Tunnell, *A Classical Diophantine Problem and Modular forms of weight 3/2*, Inventiones Math., 72 (1983), pp. 323–33.

[30] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math., 141 (1995), pp. 553–572.

[31] J. Waldspurger, *Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie*, Compositio Math., 54:2 (1985), pp. 173–242.

[32] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math., 142 (1995), pp. 443–551.

[33] X. Yuan, S. Zhang, and W. Zhang, *The Gross-Zagier formula on Shimura Curves*, Annals of Mathematics Studies Number 184, 2012.