ACTA ARITHMETICA
168.4 (2015)

On certain infinite families of imaginary quadratic fields whose Iwasawa λ-invariant is equal to 1

by

Akiko Ito (Yokohama)

1. Introduction. Throughout this paper, D will denote the fundamental discriminant of a quadratic field $\mathbb{Q}(\sqrt{D})$. Let $\chi_D := \left(\frac{D}{\cdot}\right)$ be the Kronecker character. For a prime number p, we denote by $\lambda_p(\mathbb{Q}(\sqrt{D}))$ the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}(\sqrt{D})$. If p splits in an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$, then it is known that $\lambda_p(\mathbb{Q}(\sqrt{D})) \geq 1$. We may ask how often imaginary quadratic fields with $\lambda_p = 1$ appear for a given prime number p. First, we consider the following question.

Question 1.1. *Let p be a prime number. Is the set*

$$\left\{\begin{array}{c} D\text{: the fundamental discriminant of}\\ \text{an imaginary quadratic field}\end{array} \;\middle|\; \lambda_p(\mathbb{Q}(\sqrt{D})) = 1 \text{ and } \chi_D(p) = 1\right\}$$

infinite?

For $p = 2$, Question 1.1 has an affirmative answer. In fact, we can prove this by using Kida's formula for λ_2 of imaginary quadratic fields [18].

We treat the case where $p \geq 3$. D. S. Dummit, D. Ford, H. Kisilevsky, and J. W. Sands [10], T. Fukuda and H. Taya [12], J. S. Kraft and L. C. Washington [22] and others constructed tables of λ_p for imaginary quadratic fields. For $p = 3$, T. Fukuda and H. Taya [12, p. 302] gave the following table of $\lambda_3(\mathbb{Q}(\sqrt{-d}))$ for positive square-free integers d less than 10,000,000:

λ_3	0	1	2	3	4	5
$d \equiv 0 \bmod 3$	890546 $(*)$	409063	145360	49796	16750	5517
$d \equiv 1 \bmod 3$	1327112	617243	220648	76138	25595	8666
$d \equiv 2 \bmod 3$	0	1320935	618333	225217	76691	25554

2010 *Mathematics Subject Classification*: Primary 11R11; Secondary 11R23.
Key words and phrases: imaginary quadratic field, Iwasawa λ-invariant.

DOI: 10.4064/aa168-4-1

λ_3	6	7	8	9	10	11	12	13	14	Total
$d \equiv 0 \bmod 3$	1864	613	218	50	24	8	1	1	2	1519813
$d \equiv 1 \bmod 3$	2939	912	329	112	28	12	4	2	1	2279741
$d \equiv 2 \bmod 3$	8622	2956	939	311	123	44	6	3	2	2279736

The number in $(*)$ is the number of positive square-free integers d less than 10,000,000 such that $d \equiv 0 \bmod 3$ and $\lambda_3(\mathbb{Q}(\sqrt{-d})) = 0$. It seems that the Iwasawa λ-invariants of the cyclotomic $\mathbb{Z}_3$-extensions of imaginary quadratic fields tend to be small.

Remark 1.2. Kraft and Washington [22] and J. S. Ellenberg, S. Jain, and A. Venkatesh [11] made heuristic predictions on the behavior of λ_p for imaginary quadratic fields. Ellenberg, Jain, and Venkatesh [11] conjectured the following: Let p be an odd prime number and n a non-negative integer. Among imaginary quadratic fields k in which p does not split, the probability that $\lambda_p(k) = n$ is $p^{-n} \prod_{t>n,\, t\in\mathbb{N}} (1 - p^{-t})$.

Question 1.1 was studied by D. Byeon [5]. Suppose $0 < X \in \mathbb{R}$. We denote by $S_-(X)$ the set of negative fundamental discriminants $-X < D < 0$ of quadratic fields. Byeon proved the following theorem.

Theorem 1.3 (Byeon, [5, Proposition 1.2]). *Let p be an odd prime number. Assume that there is a negative fundamental discriminant D_0 of a quadratic field which satisfies the following conditions:*

$$\text{(i) } \lambda_p(\mathbb{Q}(\sqrt{D_0})) = 1, \qquad \text{(ii) } \chi_{D_0}(p) = 1.$$

Then, for any sufficiently large $X \in \mathbb{R}$, we have

$$\sharp\{D \in S_-(X) \mid \lambda_p(\mathbb{Q}(\sqrt{D})) = 1 \text{ and } \chi_D(p) = 1\} \gg \frac{\sqrt{X}}{\log X}.$$

The assumption of the existence of D_0 is necessary for the proof. In [5], Byeon gave such a D_0 for each odd prime number by using a result of R. Gold [13, Theorem 4]. But it seems that he did not use Gold's result correctly (he did not verify the indivisibility of the class number). Therefore, we give such a D_0 in the following way.

Theorem 1.4. *Let p be an odd prime greater than 3. If $\lambda_p(\mathbb{Q}(\sqrt{1-p})) > 1$, then $\lambda_p(\mathbb{Q}(\sqrt{4-p})) = 1$.*

Example 1.5. (1) When $p = 13$, we have

$$\lambda_{13}(\mathbb{Q}(\sqrt{1-13})) = \lambda_{13}(\mathbb{Q}(\sqrt{-3})) = 2 > 1,$$
$$\lambda_{13}(\mathbb{Q}(\sqrt{4-13})) = \lambda_{13}(\mathbb{Q}(\sqrt{-1})) = 1.$$

(2) When $p = 23$, we have

$$\lambda_{23}(\mathbb{Q}(\sqrt{1-23})) = \lambda_{23}(\mathbb{Q}(\sqrt{-22})) = 2 > 1,$$
$$\lambda_{23}(\mathbb{Q}(\sqrt{4-23})) = \lambda_{23}(\mathbb{Q}(\sqrt{-19})) = 1.$$

We calculated these examples by using Mizusawa's program [24]. Since the integers $1-p$ and $4-p$ are quadratic residues modulo p, we can take $\mathbb{Q}(\sqrt{D_0})$ to be $\mathbb{Q}(\sqrt{1-p})$ or $\mathbb{Q}(\sqrt{4-p})$ when $p \geq 5$. When $p=3$, we can take $\mathbb{Q}(\sqrt{D_0})$ to be $\mathbb{Q}(\sqrt{-23})$. From Theorems 1.3 and 1.4, we obtain the following corollary.

Corollary 1.6. *Let p be an odd prime number. Then, for any sufficiently large $X \in \mathbb{R}$, we have*

$$\sharp\{D \in S_-(X) \mid \lambda_p(\mathbb{Q}(\sqrt{D})) = 1 \text{ and } \chi_D(p) = 1\} \gg \frac{\sqrt{X}}{\log X}.$$

Question 1.1 is thus answered affirmatively. Secondly, we will study a refinement of Question 1.1.

Question 1.7. *Let $p, r_1, \ldots, r_s$ and $r'_1, \ldots, r'_t$ be distinct odd prime numbers, where s and t are positive integers. Is the set*

$$\left\{ \begin{array}{c|c} D\text{: the fundamental discriminant} & \lambda_p(\mathbb{Q}(\sqrt{D})) = 1, \\ \text{of an imaginary quadratic field} & \chi_D(p) = 1, \\ & \chi_D(r_1) = \cdots = \chi_D(r_s) = 1, \text{ and} \\ & \chi_D(r'_1) = \cdots = \chi_D(r'_t) = -1 \end{array} \right\}$$

infinite?

We study the existence of infinite families of imaginary quadratic fields with $\lambda_p = 1$ under the splitting conditions of prime numbers. Results in [17, Theorem 13] and [19, Theorem] gave a hint on raising this question. We give a generalization of Theorem 1.3.

Theorem 1.8. *Let p be an odd prime number, and let $\mathfrak{S}_+$ and $\mathfrak{S}_-$ be disjoint finite sets of odd prime numbers such that $p \in \mathfrak{S}_+$. Fix (A, B) in $\{(1,8), (5,8), (8,16)\}$. Assume that there is a negative fundamental discriminant D_0 of a quadratic field which satisfies the following conditions:*

(i) *$D_0 \equiv A \bmod B$,* (ii) *$D_0 \neq -8$,* (iii) *$\lambda_p(\mathbb{Q}(\sqrt{D_0})) = 1$,*
(iv) *every $r \in \mathfrak{S}_+$ splits in $\mathbb{Q}(\sqrt{D_0})$ and every $r' \in \mathfrak{S}_-$ is inert in $\mathbb{Q}(\sqrt{D_0})$.*

Then, for any sufficiently large $X \in \mathbb{R}$, we have

$$\sharp\left\{ D \in S_-(X) \,\middle|\, \begin{array}{c} D \equiv A \bmod B, \\ \lambda_p(\mathbb{Q}(\sqrt{D})) = 1, \text{ and} \\ \text{condition } (*) \text{ holds} \end{array} \right\} \gg \frac{\sqrt{X}}{\log X},$$

where $(*)$ denotes the condition that every $r \in \mathfrak{S}_+$ splits in $\mathbb{Q}(\sqrt{D})$ and every $r' \in \mathfrak{S}_-$ is inert in $\mathbb{Q}(\sqrt{D})$.

Example 1.9. Assume $p = 3$, $\mathfrak{S}_+ := \{3\}$, $\mathfrak{S}_- := \{5\}$, and $(A, B) = (1, 8)$. In this case, we can take $D_0 = -23$, for example. It follows from Theorem 1.8 that for any sufficiently large $X \in \mathbb{R}$ we have

$$\sharp\left\{ D \in S_-(X) \;\middle|\; \begin{array}{c} D \equiv 1 \bmod 8, \\ \lambda_3(\mathbb{Q}(\sqrt{D})) = 1, \\ \chi_D(3) = 1, \text{ and } \chi_D(5) = -1 \end{array} \right\} \gg \frac{\sqrt{X}}{\log X}.$$

Since the condition that $D \equiv 1 \bmod 8$, $\chi_D(3) = 1$, and $\chi_D(5) = -1$ is equivalent to the congruence relation $D \equiv 73, 97 \bmod 120$, the above estimate implies that

$$\sharp\{D \in S_-(X) \mid D \equiv 73, 97 \bmod 120 \text{ and } \lambda_3(\mathbb{Q}(\sqrt{D})) = 1\} \gg \frac{\sqrt{X}}{\log X}.$$

In Theorems 1.3 and 1.8, we do not construct infinite families of imaginary quadratic fields with $\lambda_p = 1$ explicitly (see the proof of Theorem 1.8 in Section 3). Therefore, we consider the following problem.

Problem 1.10. *Let p be an odd prime number. Construct explicitly an infinite family of imaginary quadratic fields whose Iwasawa λ_p-invariant is equal to* 1.

We construct such fields in the following theorem. However, we do not know whether they are infinitely many or not. We denote by $h(k)$ the class number of an algebraic number field k.

Theorem 1.11. *Let p be an odd prime number, q_1 a prime factor of $p - 2$ such that $q_1^{p-1} \not\equiv 1 \bmod p^2$, and n an integer greater than* 1 *such that* $\gcd(p, n) = 1$.

(1) *Assume $p \equiv 3 \bmod 4$.*

  (i) *Suppose $p = 3$. If $3 \nmid h(\mathbb{Q}(\sqrt{1 - p^n}))$, then $\lambda_3(\mathbb{Q}(\sqrt{1 - p^n})) = 1$. Furthermore, if n_1 and n_2 are positive odd integers with $n_1, n_2 \neq 5$ such that $\mathbb{Q}(\sqrt{1 - p^{n_1}}) = \mathbb{Q}(\sqrt{1 - p^{n_2}})$, then $n_1 = n_2$.*

  (ii) *Suppose $p \neq 3$ and $2^{p-1} \not\equiv 1 \bmod p^2$. If $p \nmid h(\mathbb{Q}(\sqrt{1 - p^n}))$, then $\lambda_p(\mathbb{Q}(\sqrt{1 - p^n})) = 1$. Furthermore, if n_1 and n_2 are positive odd integers such that $\mathbb{Q}(\sqrt{1 - p^{n_1}}) = \mathbb{Q}(\sqrt{1 - p^{n_2}})$, then $n_1 = n_2$.*

  (iii) *Suppose $2^{p-1} \equiv 1 \bmod p^2$. If $p \nmid h(\mathbb{Q}(\sqrt{q_1^2 - p^n}))$, then $\lambda_p(\mathbb{Q}(\sqrt{q_1^2 - p^n})) = 1$. Furthermore, if n_1 and n_2 are positive odd composite numbers such that $\mathbb{Q}(\sqrt{q_1^2 - p^{n_1}}) = \mathbb{Q}(\sqrt{q_1^2 - p^{n_2}})$, then $n_1 = n_2$.*

(2) *Assume $p \equiv 1 \bmod 4$.*

  (i) *Suppose $2^{p-1} \not\equiv 1 \bmod p^2$. If $p \nmid h(\mathbb{Q}(\sqrt{4 - p^n}))$, then $\lambda_p(\mathbb{Q}(\sqrt{4 - p^n})) = 1$. Furthermore, if n_1 and n_2 are positive* *integers such that* $\mathbb{Q}(\sqrt{4-p^{n_1}}), \mathbb{Q}(\sqrt{4-p^{n_2}}) \neq \mathbb{Q}(\sqrt{-1})$ *and* $\mathbb{Q}(\sqrt{4-p^{n_1}}) = \mathbb{Q}(\sqrt{4-p^{n_2}})$, *then* $n_1 = n_2$.

(ii) *Suppose* $2^{p-1} \equiv 1 \bmod p^2$ *and* $4q_1^2 < p^n$. *If* $p \nmid h(\mathbb{Q}(\sqrt{4q_1^2 - p^n}))$, *then* $\lambda_p(\mathbb{Q}(\sqrt{4q_1^2 - p^n})) = 1$. *Furthermore, if* n_1 *and* n_2 *are positive composite numbers such that* $\mathbb{Q}(\sqrt{4q_1^2 - p^{n_1}}), \mathbb{Q}(\sqrt{4q_1^2 - p^{n_2}}) \neq \mathbb{Q}(\sqrt{-1})$, *and* $\mathbb{Q}(\sqrt{4q_1^2 - p^{n_1}}) = \mathbb{Q}(\sqrt{4q_1^2 - p^{n_2}})$, *then* $n_1 = n_2$.

Remark 1.12. A prime number p such that $2^{p-1} \equiv 1 \bmod p^2$ is called a *Wieferich prime.*

Remark 1.13. For a given odd prime number p with $2^{p-1} \equiv 1 \bmod p^2$, we can prove the existence of q_1 as in Theorem 1.11 as follows. Assume that $q_1^{p-1} \equiv 1 \bmod p^2$ for any prime factor q_1 of $p-2$. Then $(p-2)^{p-1} \equiv 1 \bmod p^2$. Expanding the left side of this equation, we find that

$$\begin{aligned}(p-2)^{p-1} &= \sum_{j=0}^{p-1} \binom{p-1}{j} p^j (-2)^{p-1-j} \\ &= (-2)^{p-1} + (p-1)p(-2)^{p-2} + \sum_{j=2}^{p-1} \binom{p-1}{j} p^j (-2)^{p-1-j} \\ &\equiv 2^{p-1} - p(-2)^{p-2} \bmod p^2.\end{aligned}$$

Using the assumption $2^{p-1} \equiv 1 \bmod p^2$, we obtain

$$2^{p-1} - p(-2)^{p-2} \equiv 1 - p(-2)^{p-2} \bmod p^2.$$

Thus,

$$1 \equiv 1 - p(-2)^{p-2} \bmod p^2,$$

that is, $p \mid 2$, a contradiction. Hence, there exists at least one prime factor q_1 of $p-2$ such that $q_1^{p-1} \not\equiv 1 \bmod p^2$.

Finally, as a topic relevant to Theorem 1.11, we add a result on imaginary quadratic fields whose Iwasawa λ_p-invariant is greater than 1. J. W. Sands [26] proved that there exist infinitely many imaginary quadratic fields K such that p splits in K and the Iwasawa λ_p-invariant of K is greater than 1. The outline of his proof is as follows. Fix an odd prime number p and an arbitrary integer $n \geq 2$ which is not divisible by p. Define

$$A_{p,n} := \{a \in \mathbb{Z} \mid 0 < a < 2p^n,\ p \nmid a, \text{ and } a^{p-1} \equiv 1 \bmod p^2\}.$$

He proved that p splits in $\mathbb{Q}(\sqrt{a^2 - 4p^{2n}})$ and that $\lambda_p(\mathbb{Q}(\sqrt{a^2 - 4p^{2n}})) > 1$ if $a \in A_{p,n}$ (see [26, Lemmas 3.1 and 3.2]). The cardinality of $A_{p,n}$ is $2(p-1)p^{n-2}$ (see [26, proof of Theorem 3.3]). He counted the number of imaginary quadratic fields $\mathbb{Q}(\sqrt{a^2 - 4p^{2n}})$ with $a \in A_{p,n}$ and showed that there exist at least $2(p-1)p^{n-2} - 3$ imaginary quadratic fields K such that p splits in K, $\lambda_p(K) > 1$, and the fundamental discriminant of K is greater than $-4p^{2n}$ (see [26, Theorem 3.3]). Let $n \to \infty$ in the above result. Then we find that there exist infinitely many imaginary quadratic fields K such that p splits in K and the Iwasawa λ_p-invariant of K is greater than 1 (see [26, Corollary 3.4]).

We refine Sands's proof. By studying the divisibility of the class number of the imaginary quadratic fields $\mathbb{Q}(\sqrt{1-4p^n})$, we obtain a simpler proof of his result in the following way.

Theorem 1.14. *Let p be an odd prime number and let n be an integer greater than* 1 *such that* $\gcd(p,n)=1$. *Then* $\lambda_p(\mathbb{Q}(\sqrt{1-4p^n}))>1$. *Furthermore, if n_1 and n_2 are integers greater than* 8 *such that* $\mathbb{Q}(\sqrt{1-4p^{n_1}}) = \mathbb{Q}(\sqrt{1-4p^{n_2}})$, *then* $n_1=n_2$.

For a given odd prime number p, there exist infinitely many integers n such that $n>8$ and $\gcd(p,n)=1$. We see from Theorem 1.14 that $\mathbb{Q}(\sqrt{1-4p^{n_1}}) \neq \mathbb{Q}(\sqrt{1-4p^{n_2}})$ if $n_1 \neq n_2$. Therefore,

$$\{\mathbb{Q}(\sqrt{1-4p^n}) \mid n \in \mathbb{N} \text{ such that } n>8 \text{ and } \gcd(p,n)=1\}$$

is an infinite family of imaginary quadratic fields in which p splits and whose Iwasawa λ_p-invariant is greater than 1.

This paper is organized as follows. In Section 2, we show Theorem 1.4 by using a result of Sands [26]. In Section 3, we prove Theorem 1.8 by using some property of the Fourier coefficients of Cohen's Eisenstein series of half-integral weight [7]. In Section 4, we show Theorems 1.11 and 1.14 by combining the method of proof of Theorem 1.4 and the study of divisibility of class numbers of imaginary quadratic fields.

2. Proof of Theorem 1.4.

The method of proof is based on the one in [5]. To check whether the Iwasawa λ-invariants of the cyclotomic $\mathbb{Z}_p$-extensions of imaginary quadratic fields are equal to 1, we use the following theorem.

Theorem 2.1 (Sands, [26, Proposition 2.1]). *Assume that p is an odd prime number that splits in the imaginary quadratic field K. Thus* $(p)=\wp\overline{\wp}$, *the product of prime ideals of K. Suppose that m_1 is a positive integer not divisible by p such that* $\wp^{m_1}=(\xi)$, *a principal ideal of K. Then* $\lambda_p(K)>1$ *if and only if either* $\xi^{p-1}\equiv 1 \bmod \overline{\wp}^2$ *or p divides the class number of K.*

Remark 2.2. We see from Theorem 2.1 that $\lambda_p(K)=1$ if and only if $\xi^{p-1}\not\equiv 1 \bmod \overline{\wp}^2$ and $p \nmid h(K)$. When $p\nmid h(K)$, we have $\lambda_p(K)=1$ if and only if $\xi^{p-1}\not\equiv 1 \bmod \overline{\wp}^2$. Gold proved this special case in [13], and Sands improved his result as seen above. To use their necessary and sufficient condition for $\lambda_p(K)=1$, we need to check that $p\nmid h(K)$. In [5], the above necessary and sufficient condition is used without this study.

To use Theorem 2.1, we need the following lemma.

Lemma 2.3. *Let p be an odd prime number such that $p \geq e^7$, and x_1 a positive integer such that $x_1^2 < p$. Then $p \nmid h(\mathbb{Q}(\sqrt{x_1^2 - p}))$.*

Proof. Let K be an imaginary quadratic field. The class number formula for such fields is

$$h(K) = \frac{\omega_K \sqrt{|D_K|}}{2\pi} L(1, \chi_{D_K}),$$

where ω_K is the number of roots of unity in K, D_K is the fundamental discriminant of K, and $L(s, \chi_{D_K})$ is the Dirichlet L-function. We substitute $K = \mathbb{Q}(\sqrt{x_1^2 - p})$ in this formula. Since $p \nmid h(\mathbb{Q}(\sqrt{-1})) = 1$ and $p \nmid h(\mathbb{Q}(\sqrt{-3})) = 1$, we may assume $\mathbb{Q}(\sqrt{x_1^2 - p}) \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, that is, we may assume $\omega_{\mathbb{Q}(\sqrt{x_1^2 - p})} = 2$. Substituting this in the class number formula, we get

$$h\big(\mathbb{Q}\big(\sqrt{x_1^2 - p}\big)\big) = \frac{\sqrt{|D_{\mathbb{Q}(\sqrt{x_1^2 - p})}|}}{\pi} L(1, \chi_{D_{\mathbb{Q}(\sqrt{x_1^2 - p})}}).$$

From

$$|D_{\mathbb{Q}(\sqrt{x_1^2 - p})}| \leq 4|x_1^2 - p| = 4(p - x_1^2) < 4p,$$

we see that

$$h\big(\mathbb{Q}\big(\sqrt{x_1^2 - p}\big)\big) < \frac{2\sqrt{p}}{\pi} L(1, \chi_{D_{\mathbb{Q}(\sqrt{x_1^2 - p})}}).$$

We have

$$L(1, \chi_{D_K}) \leq \tfrac{1}{2} \log |D_K| + \log\log |D_K| + 2.8$$

(see [8, Proposition 10.3.16]). Using this inequality, we obtain

$$\begin{aligned}
(2.1) \qquad & \frac{2\sqrt{p}}{\pi} L(1, \chi_{D_{\mathbb{Q}(\sqrt{x_1^2 - p})}}) \\
& \leq \frac{2\sqrt{p}}{\pi} \left\{ \frac{1}{2} \log |D_{\mathbb{Q}(\sqrt{x_1^2 - p})}| + \log\log |D_{\mathbb{Q}(\sqrt{x_1^2 - p})}| + 2.8 \right\} \\
& < \frac{2\sqrt{p}}{\pi} \left\{ \frac{1}{2} \log 4p + \log\log 4p + 2.8 \right\} \\
& = \frac{2\sqrt{p}}{\pi} \left\{ \frac{1}{2} \cdot 2\log 2 + \frac{1}{2} \log p + \log(2\log 2 + \log p) + 2.8 \right\} \\
& = \frac{2\sqrt{p}}{\pi} \left\{ \frac{1}{2} \log p + (\log 2 + \log(2\log 2 + \log p) + 2.8) \right\}.
\end{aligned}$$

We now prove that

$$(2.2) \qquad \log 2 + \log(2\log 2 + \log p) + 2.8 < \log p \quad \text{when } p \geq e^7.$$

Indeed, let

$$f_1(X) := \log X - 4 - \log(2\log 2 + \log X).$$

From

$$f_1'(X) = \frac{1}{X} - \frac{1/X}{2\log 2 + \log X} = \frac{1}{X}\left(\frac{2\log 2 + \log X - 1}{2\log 2 + \log X}\right),$$

we see that $f_1'(X) > 0$ when $X \geq e$. Thus, $f_1(X)$ increases when $X \geq e$. For $X = e^7$, we have

$$\begin{aligned} f_1(e^7) &= \log e^7 - 4 - \log(2\log 2 + \log e^7) \\ &= 7 - 4 - \log(2\log 2 + 7) = 3 - \log(2\log 2 + 7) \\ &> 3 - \log(2+7) = 3 - \log 9 = \log\frac{e^3}{9} > 0. \end{aligned}$$

Hence, $f_1(X) > 0$ when $X \geq e^7$, that is,

$$\log X > 4 + \log(2\log 2 + \log X) \quad \text{when } X \geq e^7.$$

Since $\log 2 + 2.8 < 4$, we have

$$4 + \log(2\log 2 + \log X) > \log 2 + \log(2\log 2 + \log X) + 2.8.$$

Hence,

$$\log p > \log 2 + \log(2\log 2 + \log p) + 2.8 \quad \text{when } p \geq e^7,$$

proving (2.2).

Substituting this in (2.1), we see that

$$\begin{aligned} \frac{2\sqrt{p}}{\pi}L(1, \chi_{D_{\mathbb{Q}(\sqrt{x_1^2-p})}}) &< \frac{2\sqrt{p}}{\pi}\left(\frac{1}{2}\log p + \log p\right) \\ &= \frac{2\sqrt{p}}{\pi}\,\frac{3}{2}\log p = \frac{3\sqrt{p}}{\pi}\log p \quad \text{when } p \geq e^7. \end{aligned} \tag{2.3}$$

Next, we prove that

$$\log p < \sqrt{p} \quad \text{when } p \geq e^2. \tag{2.4}$$

In fact, let $f_2(X) := \sqrt{X} - \log X$. Since

$$f_2'(X) = \frac{1}{2}X^{-1/2} - \frac{1}{X} = \frac{1}{2\sqrt{X}} - \frac{1}{X} = \frac{\sqrt{X} - 2}{2X},$$

we see that $f_2'(X) > 0$ when $X > 4$. Thus, $f_2(X)$ increases when $X > 4$. As

$$f_2(e^2) = \sqrt{e^2} - \log e^2 = e - 2 > 0,$$

we have $f_2(X) > 0$ when $X \geq e^2$, proving (2.4).

Substituting this in (2.3), we obtain

$$\begin{aligned}\frac{2\sqrt{p}}{\pi}L(1,\chi_{D_{\mathbb{Q}(\sqrt{x_1^2-p})}}) &< \frac{3\sqrt{p}}{\pi}\log p\\ &< \frac{3\sqrt{p}}{\pi}\sqrt{p}=\frac{3p}{\pi}<p \quad \text{when } p\ge e^7.\end{aligned}$$

This implies that $h(\mathbb{Q}(\sqrt{x_1^2-p}))<p$ when $p\ge e^7$, that is, $p\nmid h(\mathbb{Q}(\sqrt{x_1^2-p}))$ when $p\ge e^7$. ■

Using the Kash program, we can check that the class numbers of $\mathbb{Q}(\sqrt{1-p})$ and $\mathbb{Q}(\sqrt{4-p})$ are not divisible by p when $3<p<e^7$. From this and Lemma 2.3, we get the following lemma.

Lemma 2.4. *Let p be an odd prime number greater than* 3. *Then the class numbers of $\mathbb{Q}(\sqrt{1-p})$ and $\mathbb{Q}(\sqrt{4-p})$ are not divisible by p.*

We now show Theorem 1.4 by using Lemma 2.4.

Proof of Theorem 1.4. First, we analyse $\mathbb{Q}(\sqrt{1-p})$. Suppose that $\lambda_p(\mathbb{Q}(\sqrt{1-p}))>1$. We can write

$$\wp_1\overline{\wp_1}=(p)=(1+\sqrt{1-p})(1-\sqrt{1-p})$$

in $\mathbb{Q}(\sqrt{1-p})$, where $\wp_1$ denotes the prime ideal of $\mathbb{Q}(\sqrt{1-p})$ over p, and $\overline{\wp_1}$ denotes the complex conjugate of $\wp_1$. Since $p\nmid(1+\sqrt{1-p})$ and $p\nmid(1-\sqrt{1-p})$, we may assume $\wp_1=(1+\sqrt{1-p})$ and $\overline{\wp_1}=(1-\sqrt{1-p})$. Then $\wp_1^2$ is a principal ideal. Applying Theorem 2.1 for $K=\mathbb{Q}(\sqrt{1-p})$, $m_1=2$, and $\xi=(1+\sqrt{1-p})^2$, we see from Lemma 2.4 that $\lambda_p(\mathbb{Q}(\sqrt{1-p}))>1$ if and only if

$$((1+\sqrt{1-p})^2)^{p-1}\equiv 1 \bmod \overline{\wp_1}^2.$$

This is equivalent to

$$(1+\sqrt{1-p})^{2(p-1)}(1+\sqrt{1-p})^2-(1+\sqrt{1-p})^2\equiv 0 \bmod \wp_1^2\overline{\wp_1}^2,$$

that is,

$$(1+\sqrt{1-p})^{2p}-(1+\sqrt{1-p})^2\equiv 0 \bmod p^2. \tag{2.5}$$

Expanding the left side, we obtain

$$\begin{aligned}&(1+\sqrt{1-p})^{2p}-(1+\sqrt{1-p})^2\\ &\quad=\Big\{\sum_{j=0}^{p}\binom{2p}{2j}(1-p)^j\Big\}+\sqrt{1-p}\Big\{\sum_{j=0}^{p-1}\binom{2p}{2j+1}(1-p)^j\Big\}\\ &\quad\quad-(2-p+2\sqrt{1-p}).\end{aligned} \tag{2.6}$$

Note that

$$(1-p)^j=\sum_{i=0}^{j}\binom{j}{i}(-p)^i=1+\binom{j}{1}(-p)+\sum_{i=2}^{j}\binom{j}{i}(-p)^i\equiv 1-jp \bmod p^2.$$

Substituting this in (2.6), we obtain

$$\begin{aligned}
&(1+\sqrt{1-p})^{2p}-(1+\sqrt{1-p})^2\\
&\quad\equiv\Big\{\sum_{j=0}^{p}\binom{2p}{2j}(1-jp)\Big\}+\sqrt{1-p}\Big\{\sum_{j=0}^{p-1}\binom{2p}{2j+1}(1-jp)\Big\}\\
&\qquad-(2-p+2\sqrt{1-p})\\
&\quad\equiv\sum_{j=0}^{p}\binom{2p}{2j}-p\sum_{j=0}^{p}\binom{2p}{2j}j+\sqrt{1-p}\Big\{\sum_{j=0}^{p-1}\binom{2p}{2j+1}-p\sum_{j=0}^{p-1}\binom{2p}{2j+1}j\Big\}\\
&\qquad-(2-p+2\sqrt{1-p})\bmod p^2.
\end{aligned}$$

Since

$$\sum_{j=0}^{p}\binom{2p}{2j}=\sum_{j=0}^{p-1}\binom{2p}{2j+1}=2^{2p-1},\qquad \sum_{j=0}^{p}\binom{2p}{2j}j=2^{2p-2}p,$$

and

$$\sum_{j=0}^{p-1}\binom{2p}{2j+1}j=2^{2p-2}(p-1),$$

we have

$$\begin{aligned}
&(1+\sqrt{1-p})^{2p}-(1+\sqrt{1-p})^2\\
&\quad\equiv 2^{2p-1}-2^{2p-2}p^2+\sqrt{1-p}\{2^{2p-1}-2^{2p-2}p(p-1)\}-(2-p+2\sqrt{1-p})\\
&\quad\equiv 2^{2p-1}+\sqrt{1-p}(2^{2p-1}+2^{2p-2}p)-(2-p+2\sqrt{1-p})\\
&\quad\equiv(2^{2p-1}-2+p)+\sqrt{1-p}(2^{2p-1}+2^{2p-2}p-2)\bmod p^2.
\end{aligned}$$

From this and (2.5), we obtain

$$2^{2p-1}-2+p\equiv 0\bmod p^2 \tag{2.7}$$

and

$$2^{2p-1}+2^{2p-2}p-2\equiv 0\bmod p^2. \tag{2.8}$$

In fact, (2.7) implies (2.8), because when $2^{2p-1}\equiv 2-p\bmod p^2$, we have

$$\begin{aligned}
2^{2p-1}+2^{2p-2}p-2&\equiv 2-p+2^{2p-2}p-2\\
&\equiv -p+2^{2p-2}p\equiv p(2^{2p-2}-1)\bmod p^2,
\end{aligned}$$

and since $2^{2p-2}-1\equiv 0\bmod p$, we obtain (2.8).

Thus, $\lambda_p(\mathbb{Q}(\sqrt{1-p}))>1$ if and only if

$$2^{2p-1}-2+p\equiv 0\bmod p^2.$$

Secondly, we analyse $\mathbb{Q}(\sqrt{4-p})$. We can write

$$\wp_2\overline{\wp_2} = (p) = (2+\sqrt{4-p})(2-\sqrt{4-p})$$

in $\mathbb{Q}(\sqrt{4-p})$, where $\wp_2$ denotes the prime ideal of $\mathbb{Q}(\sqrt{4-p})$ over p, and $\overline{\wp_2}$ denotes the complex conjugate of $\wp_2$. Since $p \nmid (2+\sqrt{4-p})$ and $p \nmid (2-\sqrt{4-p})$, we may assume $\wp_2 = (2+\sqrt{4-p})$ and $\overline{\wp_2} = (2-\sqrt{4-p})$. Then $\wp_2^2$ is a principal ideal. Applying Theorem 2.1 for $K = \mathbb{Q}(\sqrt{4-p})$, $m_1 = 2$, and $\xi = (2+\sqrt{4-p})^2$, we see from Lemma 2.4 that $\lambda_p(\mathbb{Q}(\sqrt{4-p})) = 1$ if and only if

$$((2+\sqrt{4-p})^2)^{p-1} \not\equiv 1 \bmod \overline{\wp_2}^2. \tag{2.9}$$

We will prove that this is equivalent to

$$2^{4p-1} - 2^3 + p \not\equiv 0 \bmod p^2$$

or

$$2^{4p-2} + 2^{4p-5}p - 2^2 \not\equiv 0 \bmod p^2.$$

Indeed, (2.9) is equivalent to

$$(2+\sqrt{4-p})^{2(p-1)}(2+\sqrt{4-p})^2 - (2+\sqrt{4-p})^2 \not\equiv 0 \bmod \wp_2^2\overline{\wp_2}^2,$$

that is,

$$(2+\sqrt{4-p})^{2p} - (2+\sqrt{4-p})^2 \not\equiv 0 \bmod p^2. \tag{2.10}$$

Expanding the left side, we obtain

$$\begin{aligned}
&(2+\sqrt{4-p})^{2p} - (2+\sqrt{4-p})^2 \\
&\quad = \sum_{j=0}^{p}\binom{2p}{2j}(4-p)^j 2^{2p-2j} + \sqrt{4-p}\left\{\sum_{j=0}^{p-1}\binom{2p}{2j+1}(4-p)^j 2^{2p-(2j+1)}\right\} \\
&\qquad - (4+4\sqrt{4-p}+4-p) \\
&\quad \equiv \sum_{j=0}^{p}\binom{2p}{2j}(4^j - 4^{j-1}jp)2^{2p-2j} \\
&\qquad + \sqrt{4-p}\left\{\sum_{j=0}^{p-1}\binom{2p}{2j+1}(4^j - 4^{j-1}jp)2^{2p-2j-1}\right\} - (8-p+4\sqrt{4-p}) \\
&\quad \equiv \sum_{j=0}^{p}\binom{2p}{2j}(2^{2p} - 2^{2p-2}jp) + \sqrt{4-p}\left\{\sum_{j=0}^{p-1}\binom{2p}{2j+1}(2^{2p-1} - 2^{2p-3}jp)\right\} \\
&\qquad - (8-p+4\sqrt{4-p})
\end{aligned}$$

$$\begin{aligned}
&\equiv 2^{2p}\sum_{j=0}^{p}\binom{2p}{2j} - 2^{2p-2}p\sum_{j=0}^{p} j\binom{2p}{2j}\\
&\quad + \sqrt{4-p}\biggl\{2^{2p-1}\sum_{j=0}^{p-1}\binom{2p}{2j+1} - 2^{2p-3}p\sum_{j=0}^{p-1} j\binom{2p}{2j+1}\biggr\}\\
&\quad - (8-p+4\sqrt{4-p})\\
&\equiv 2^{2p}2^{2p-1} - 2^{2p-2}p\cdot 2^{2p-2}p\\
&\quad + \sqrt{4-p}\{2^{2p-1}2^{2p-1} - 2^{2p-3}p(p-1)2^{2p-2}\} - 8 + p - 4\sqrt{4-p}\\
&\equiv 2^{4p-1} + \sqrt{4-p}\{2^{4p-2} - (-1)2^{2p-3}2^{2p-2}p\} - 8 + p - 4\sqrt{4-p}\\
&\equiv (2^{4p-1} - 8 + p) + \sqrt{4-p}(2^{4p-2} + 2^{4p-5}p - 4) \not\equiv 0 \bmod p^2.
\end{aligned}$$

Thus,

$$2^{4p-1} - 2^3 + p \not\equiv 0 \bmod p^2$$

or

$$2^{4p-2} + 2^{4p-5}p - 2^2 \not\equiv 0 \bmod p^2.$$

On the other hand, we have proved that the assumption $\lambda_p(\mathbb{Q}(\sqrt{1-p})) > 1$ implies

$$2^{2p-1} \equiv 2 - p \bmod p^2.$$

Substituting this in $2^{4p-1} - 2^3 + p$, we get

$$\begin{aligned}
2^{4p-1} - 2^3 + p &\equiv 2^{2p-1}2^{2p-1}2 - 8 + p \equiv 2(2-p)^2 - 8 + p\\
&\equiv 2(p^2 - 4p + 4) - 8 + p \equiv 2p^2 - 8p + 8 - 8 + p\\
&\equiv 2p^2 - 7p \equiv -7p \bmod p^2.
\end{aligned}$$

When $p \neq 7$, we find that

$$2^{4p-1} - 2^3 + p \not\equiv 0 \bmod p^2.$$

Therefore, if $p \neq 7$ and $\lambda_p(\mathbb{Q}(\sqrt{1-p})) > 1$, then $\lambda_p(\mathbb{Q}(\sqrt{4-p})) = 1$.

When $p = 7$, we see that

$$2^{2p-1} - 2 + p = 2^{13} + 5 = 8197 \not\equiv 0 \bmod 7^2.$$

Hence also $\lambda_7(\mathbb{Q}(\sqrt{1-7})) = \lambda_7(\mathbb{Q}(\sqrt{-6})) = 1$. ■

3. Proof of Theorem 1.8. The method of proof is based on [5]. We use some property of the Fourier coefficients of Eisenstein series of half-integral weight constructed by H. Cohen [7]. The idea of the proof is used widely in the study of indivisibility of the class number of quadratic fields (cf. W. Kohnen and K. Ono [21], K. Ono [25], D. Byeon [2, 3, 4], I. Kimura [19], etc.). First, we outline the proof. To check whether the Iwasawa λ-invariants of the cyclotomic $\mathbb{Z}_p$-extensions of imaginary quadratic fields are equal to 1, we use the following proposition.

Proposition 3.1 (cf. [5, Proposition 2.3]). *Let p be an odd prime number and D the fundamental discriminant of the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ such that $\chi_D(p) = 1$. Then $L(1-p,\chi_D)/p$ is p-integral. Furthermore,*

$$\lambda_p(\mathbb{Q}(\sqrt{D})) = 1 \quad \textit{if and only if} \quad \frac{L(1-p,\chi_D)}{p} \not\equiv 0 \bmod p,$$

where $L(s,\chi_D)$ denotes the Dirichlet L-function.

To show this, we need some property of the Kubota–Leopoldt p-adic L-function [28, Lemma 1] and [10, Proposition 5.1]. We can check from Proposition 3.1 whether $\lambda_p(\mathbb{Q}(\sqrt{D})) = 1$ or not by studying the congruence modulo p^2 of $L(1-p,\chi_D)$. We can consider $L(1-p,\chi_D)$ as a Fourier coefficient of an Eisenstein series of half-integral weight constructed by Cohen [7]. Let us now define this Eisenstein series.

Let $\mathfrak{r}$ be an integer greater than 1 and N a non-negative integer. If $(-1)^{\mathfrak{r}}N \not\equiv 0, 1 \bmod 4$, then let $H(\mathfrak{r},N) := 0$. If $N = 0$, then let $H(\mathfrak{r},0) := \zeta(1-2\mathfrak{r}) = -B_{2\mathfrak{r}}/2\mathfrak{r}$, where $\zeta(s)$ denotes the Riemann zeta-function and $B_{\mathfrak{r}}$ denotes the Bernoulli numbers. If N is a positive integer and $(-1)^{\mathfrak{r}}N = Dm^2$ where D is the fundamental discriminant of $\mathbb{Q}(\sqrt{D})$ and m is a positive integer, then define

$$H(\mathfrak{r},N) := L(1-\mathfrak{r},\chi_D)\sum_{d|m}\mu(d)\chi_D(d)d^{\mathfrak{r}-1}\sigma_{2\mathfrak{r}-1}(m/d),$$

where $\mu(\cdot)$ is the Möbius function and $\sigma_\nu(\cdot)$ the divisor function, $\sigma_\nu(m) := \sum_{d|m} d^\nu$. Let $M_k(\mathit{\Gamma}_0(N_1),\chi)$ denote the space of modular forms of weight k on the congruence subgroup $\mathit{\Gamma}_0(N_1)$ with Dirichlet character χ. Cohen proved the following proposition.

Proposition 3.2 (Cohen, [7]). *If $F_{\mathfrak{r}}(z) := \sum_{N=0}^{\infty} H(\mathfrak{r},N)q^N$, then $F_{\mathfrak{r}}(z)$ is in $M_{\mathfrak{r}+1/2}(\mathit{\Gamma}_0(4),\chi_0)$, where $q := e^{2\pi iz}$ and χ_0 denotes the trivial character modulo* 4.

In our proof, we use this Eisenstein series. Let p be an odd prime number. Set

$$G_p(z) := \frac{1}{p}F_p(z).$$

We see from Proposition 3.2 that

$$G_p(z) = \sum_{N=0}^{\infty}\frac{H(p,N)}{p}q^N \in M_{p+1/2}(\mathit{\Gamma}_0(4),\chi_0).$$

Assume that N is a positive integer and that $(-1)^pN = Dm^2$ for some fundamental discriminant D of an imaginary quadratic field such that $\chi_D(p) = 1$

and some positive integer m. If

$$H(p,N)/p \not\equiv 0 \bmod p,$$

then

$$\lambda_p(\mathbb{Q}(\sqrt{D})) = 1$$

by Proposition 3.1. Considering $L(1-p,\chi_D)/p$ as a Fourier coefficient of the Eisenstein series $G_p(z)$, we will now use properties of modular forms to obtain Theorem 1.8.

3.1. Proof of Theorem 1.8. The proof relies on Sturm's theorem on congruences of modular forms [27]. In Section 3.1.1, we state this theorem. In Section 3.1.2, we prepare a lemma. In Section 3.1.3, we prove Theorem 1.8.

3.1.1. *Sturm's theorem.* Let

$$g_1(z) = \sum_{N=0}^{\infty} a_1(N) q^N$$

be any formal power series of the indeterminate q with rational integer coefficients. We define the *order* $\operatorname{ord}_{p_1}(g_1)$ of $g_1(z)$ at a prime number p_1 by

$$\operatorname{ord}_{p_1}(g_1) := \min\{N \mid a_1(N) \not\equiv 0 \bmod p_1\}.$$

Let

$$g_2(z) = \sum_{N=0}^{\infty} a_2(N) q^N$$

be another formal power series with rational integer coefficients and m_2 a rational integer. We define $g_1(z) \equiv g_2(z) \bmod m_2$ if and only if $a_1(N) \equiv a_2(N) \bmod m_2$ for all non-negative integers N. J. Sturm proved the following theorem on congruences of modular forms.

THEOREM 3.3 (Sturm, [27]). *Let p_1 be a prime number, $k \in \frac{1}{2}\mathbb{Z}$, N_1 a positive integer (if $k \notin \mathbb{Z}$, we assume that $4 \mid N_1$), and χ a Dirichlet character. If $g(z) \in M_k(\Gamma_0(N_1),\chi)$ has rational integer coefficients and*

$$\operatorname{ord}_{p_1}(g) > \frac{k}{12}[\Gamma_0(1) : \Gamma_0(N_1)] = \frac{k}{12} N_1 \prod_{q_2 \mid N_1,\, q_2 \colon \mathit{prime}} (1 + q_2^{-1}),$$

then $g(z) \equiv 0 \bmod p_1$.

3.1.2. *A preliminary lemma*

LEMMA 3.4. *Let p be an odd prime number and*

$$\mathcal{A}_1 := \left\{ N \in \mathbb{N} \,\middle|\, \left(\frac{-N}{p}\right) = 1 \right\}.$$

Then there exists an integer $\alpha(p)$ coprime to p such that

$$\alpha(p) H(p,N)/p \in \mathbb{Z} \quad \textit{for all } N \in \mathcal{A}_1.$$

Proof. Assume $N \in \mathcal{A}_1$. If $(-1)^p N = Dm^2$ where D is the fundamental discriminant of $\mathbb{Q}(\sqrt{D})$ and m is a positive integer, then

$$\frac{H(p,N)}{p} = \frac{L(1-p,\chi_D)}{p} \sum_{d|m} \mu(d)\chi_D(d)d^{p-1}\sigma_{2p-1}(m/d)$$

by the definition of $H(p,N)$. Since $\sum_{d|m} \mu(d)\chi_D(d)d^{p-1}\sigma_{2p-1}(m/d)$ is an integer, we check the value of $L(1-p,\chi_D)/p$. Note that $\chi_D(p) = 1$. Hence, $L(1-p,\chi_D)/p$ is p-integral by Proposition 3.1. Therefore, we need to check $L(1-p,\chi_D)$. It can be represented by using the generalized Bernoulli number $B(p,\chi_D)$ as follows:

$$L(1-p,\chi_D) = -B(p,\chi_D)/p.$$

The numbers $B(p,\chi_D)/p$ are always integers unless $D = -4$ or $D = \pm p_2$, in which case they have denominator 2 or p_2 respectively, where p_2 is an odd prime number such that $2p/(p_2-1)$ is an odd integer (cf. [6]). Let m_3 be a positive integer. If $2p/(m_3-1)$ is an odd integer, then $m_3 = 3$ or $m_3 = 2p+1$. Therefore, we can take $\alpha(p) = 6(2p+1)$ when $p \neq 3$. When $p = 3$, we can take $\alpha(p) = 2(2p+1) = 14$ because $\chi_D(p) = 1$. ∎

3.1.3. *Proof of Theorem 1.8.* Let $\mathfrak{S}_+ := \{p, r_1, \ldots, r_s\}$ and $\mathfrak{S}_- := \{r_1', \ldots, r_t'\}$, where s and t are positive integers. Suppose Q is a prime number such that $Q \notin \mathfrak{S}_+ \cup \mathfrak{S}_-$, $\left(\frac{-D_0}{Q}\right) = -1$, and $Q \equiv 1 \bmod 8$. The integer $\alpha(p)$ is the one in Lemma 3.4. Let p_3 be an odd prime number and $\delta := \pm 1$. Define $G_1(z) \in M_{p+1/2}(\Gamma_0(4p_3^2), \chi_0)$ by

$$G_1(z) := \alpha(p)G_p(z) \otimes \left(\frac{\cdot}{p_3}\right) = \alpha(p) \sum_{N=0}^{\infty} \left(\frac{N}{p_3}\right) \frac{H(p,N)}{p} q^N$$

and $G_2(z) \in M_{p+1/2}(\Gamma_0(4p_3^4), \chi_0)$ by

$$G_2(z) := \frac{1}{2}\left\{G_1(z) \otimes \left(\frac{\cdot}{p_3}\right) + \delta G_1(z)\right\} = \alpha(p) \sum_{\substack{(\frac{N}{p_3})=\delta}}^{\infty} \frac{H(p,N)}{p} q^N.$$

Repeating this process for prime numbers in $\mathfrak{S}_+ \cup \mathfrak{S}_- \cup \{Q\}$, we define $G_3(z) \in M_{p+1/2}(\Gamma_0(4P_1), \chi_0)$ by

$$G_3(z) := \alpha(p) \sum_{N \in \mathcal{A}_2} \frac{H(p,N)}{p} q^N,$$

where $P_1 := \prod_{r \in \mathfrak{S}_+ \cup \mathfrak{S}_- \cup \{Q\}} r^4$ and

$$\mathcal{A}_2 := \left\{ N \in \mathbb{N} \;\middle|\; \begin{array}{c} \left(\frac{-N}{r}\right) = 1 \text{ for all } r \in \mathfrak{S}_+ \text{ and} \\ \left(\frac{-N}{r'}\right) = -1 \text{ for all } r' \in \mathfrak{S}_- \cup \{Q\} \end{array} \right\}.$$

Define $G_4(z) \in M_{p+1/2}(\Gamma_0(4 \cdot 8^2 P_1), \chi_0)$ by

$$G_4(z) := G_3(z) \otimes \chi_8 = \alpha(p) \sum_{N \equiv 3,7 \bmod 8,\, N \in \mathcal{A}_2}^{\infty} \chi_8(N) \frac{H(p,N)}{p} q^N$$

and $G_5(z) \in M_{p+1/2}(\Gamma_0(4 \cdot 8^4 P_1), \chi_0)$ by

$$G_5(z) := \frac{1}{2}\{G_4(z) \otimes \chi_8 + \delta G_4(z)\} = \alpha(p) \sum_{N \equiv -A_1 \bmod 8,\, N \in \mathcal{A}_2}^{\infty} \frac{H(p,N)}{p} q^N,$$

where χ_8 denotes the Kronecker character modulo 8, $A_1 := 1$ if $\delta = 1$, and $A_1 := 5$ otherwise. Let $\psi : (\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{C}^\times$ be the Dirichlet character defined by $\psi(1) = 1$ and $\psi(3) = -1$. Define $G_6(z) \in M_{p+1/2}(\Gamma_0(4^3 P_1), \chi_0)$ by

$$G_6(z) := G_3(z) + G_3(z) \otimes \psi = \alpha(p) \sum_{N \equiv 0 \bmod 4,\, N \in \mathcal{A}_2}^{\infty} \frac{H(p,N)}{p} q^N.$$

Using the U-operator and V-operator, define $G_7(z) \in M_{p+1/2}(\Gamma_0(4^5 P_1), \chi_0)$ by

$$\begin{aligned} G_7(z) &:= (U_2 \mid V_2 \mid G_6)(z) - (U_4 \mid V_4 \mid G_6)(z) \\ &= \alpha(p) \sum_{N \equiv 8 \bmod 16,\, N \in \mathcal{A}_2}^{\infty} \frac{H(p,N)}{p} q^N. \end{aligned}$$

For the convenience of the reader, we recall the definition of the modular forms $(U_{p_1} \mid g)(z)$ and $(V_{p_1} \mid g)(z) \in M_k\big(\Gamma_0(p_1 N_1), \big(\frac{4p_1}{\cdot}\big)\big)$, where p_1 is a prime number, $k \in \frac{1}{2}\mathbb{Z}$, N_1 a positive integer with $4 \,|\, N_1$, and $g(z) := \sum_{N=1}^{\infty} a(N) q^N \in M_k(\Gamma_0(N_1), \chi_0)$:

$$(U_{p_1} \mid g)(z) := \sum_{N=1}^{\infty} a(p_1 N) q^N, \qquad (V_{p_1} \mid g)(z) := \sum_{N=1}^{\infty} a(N) q^{p_1 N}.$$

Then we can construct the modular form

$$G(z) := \alpha(p) \sum_{N \equiv -A \bmod B,\, N \in \mathcal{A}_2}^{\infty} \frac{H(p,N)}{p} q^N \in M_{p+1/2}(\Gamma_0(P_2), \chi_0),$$

where (A, B) is a pair of fixed integers in $\{(1,8), (5,8), (8,16)\}$, $P_2 := 4^5 P_1$ if $(A,B) = (8,16)$, and $P_2 := 4^7 P_1$ otherwise (see the definition of $G_5(z)$ and $G_7(z)$). If $(-1)^p N = -N = Dm^2$ for the fundamental discriminant D of an imaginary quadratic field and some positive integer m, it follows that $D \equiv A \bmod B$ from $N \equiv -A \bmod B$, and that

$$\left(\frac{D}{p}\right) = \left(\frac{D}{r_i}\right) = 1 \quad \text{and} \quad \left(\frac{D}{Q}\right) = \left(\frac{D}{r'_j}\right) = -1$$

because

$$\left(\frac{-N}{p}\right) = \left(\frac{-N}{r_i}\right) = 1 \quad \text{and} \quad \left(\frac{-N}{Q}\right) = \left(\frac{-N}{r'_j}\right) = -1,$$

where i runs over $1, \dots, s$ and j runs over $1, \dots, t$. We denote

$$\kappa := 1 + 2^{m_4}(2p+1) \prod_{r \in \mathfrak{S}_+ \cup \mathfrak{S}_- \cup \{Q\}} r^3(r+1),$$

where $m_4 := 10$ if $A = 1, 5$ and $m_4 := 6$ otherwise. Set

$\mathcal{A}_3 := \{N \in \mathcal{A}_2 \mid 1 \le N \le \kappa \text{ and } -N \equiv A \bmod B\}$,

$\mathfrak{S}_p := \{D_N\colon \text{the fundamental discriminant of } \mathbb{Q}(\sqrt{-N}) \mid N \in \mathcal{A}_3\}$.

It is essential for the proof of Theorem 1.8 to show the following theorem.

Theorem 3.5. *Let l be an odd prime number satisfying the following conditions:*

(i) $\kappa < l$,
(ii) $l \equiv 1 \bmod P_3$,
(iii) $\chi_D(l) = -1$ *for all* $D \in \mathfrak{S}_p \cup \{D_0\}$,

where $P_3 := B \prod_{r \in \mathfrak{S}_+ \cup \mathfrak{S}_- \cup \{Q\}} r$. *Then there exists a positive integer N_l satisfying the following conditions:*

(I) $1 \le N_l \le l\kappa$,
(II) $l \nmid N_l$,
(III) $lN_l \equiv -A \bmod B$,
(IV) $lN_l \in \mathcal{A}_2$,
(V) $H(p, lN_l)/p \not\equiv 0 \bmod p$.

We prove the existence of prime numbers l satisfying the above conditions later (see Lemma 3.7).

Proof of Theorem 3.5. By using the U-operator and V-operator, we construct the modular form

$$G_l(z) := (U_l \mid G)(z) - 3(V_l \mid G)(z) \in M_{p+1/2}\left(\Gamma_0(lP_2), \left(\frac{4l}{\cdot}\right)\right).$$

The coefficient $b(N)$ of q^N in $G_l(z)$ is represented as follows:

$$b(N) = \frac{\alpha(p)}{p}\{H(p, lN) - 3H(p, N/l)\}.$$

First, we treat the case where $l \mid N$. We can write $N = lN'$ for some integer N'. Then

$$b(N) = \frac{\alpha(p)}{p}\{H(p, l^2N') - 3H(p, N')\}.$$

If $N' \notin \mathcal{A}_2$, then $b(N) = 0$. If $N' \equiv -A \bmod B$, $N' \in \mathcal{A}_2$, and $1 \le N' \le \kappa$, we can show $b(N) \equiv 0 \bmod p$ as follows. We write $-N' = D_{N'}m'^2$ for the fundamental discriminant $D_{N'}$ of an imaginary quadratic field and some positive integer m'. Then

$$b(N) = \frac{\alpha(p)}{p}\{H(p, -D_{N'}(lm')^2) - 3H(p, -D_{N'}m'^2)\}.$$

We see from the definition of $H(p, N)$ that

$$\tag{3.1} \begin{aligned} &\frac{\alpha(p)H(p, -D_{N'}(lm')^2)}{p} \\ &\qquad = \frac{\alpha(p)H(p, -D_{N'})}{p}\left\{\sum_{d|lm'} \mu(d)\chi_{D_{N'}}(d)d^{p-1}\sigma_{2p-1}(lm'/d)\right\}. \end{aligned}$$

Since $l > \kappa$ and $\kappa \ge N'$, we have $\gcd(l, m') = 1$. Thus,

$$\begin{aligned} &\sum_{d|lm'} \mu(d)\chi_{D_{N'}}(d)d^{p-1}\sigma_{2p-1}(lm'/d) \\ &= \sum_{d|m'}\{\mu(d)\chi_{D_{N'}}(d)d^{p-1}\sigma_{2p-1}(lm'/d)+\mu(ld)\chi_{D_{N'}}(ld)l^{p-1}d^{p-1}\sigma_{2p-1}(m'/d)\} \\ &= \sum_{d|m'}\{(1+l^{2p-1})\mu(d)\chi_{D_{N'}}(d)d^{p-1}\sigma_{2p-1}(m'/d) \\ &\qquad\qquad - \mu(d)\chi_{D_{N'}}(l)\chi_{D_{N'}}(d)l^{p-1}d^{p-1}\sigma_{2p-1}(m'/d)\} \\ &= (1+l^{2p-1}+l^{p-1})\sum_{d|m'} \mu(d)\chi_{D_{N'}}(d)d^{p-1}\sigma_{2p-1}(m'/d). \end{aligned}$$

Substituting this in (3.1), we obtain

$$\frac{\alpha(p)H(p, -D_{N'}(lm')^2)}{p} = (1 + l^{2p-1} + l^{p-1})\frac{\alpha(p)H(p, -D_{N'}m'^2)}{p}.$$

We see from the assumption $l \equiv 1 \bmod p$ that

$$(1 + l^{2p-1} + l^{p-1})\frac{\alpha(p)H(p, -D_{N'}m'^2)}{p} \equiv \frac{3\alpha(p)H(p, -D_{N'}m'^2)}{p} \bmod p.$$

Hence,

$$b(N) \equiv 0 \bmod p.$$

Therefore, if $l \mid N$ and $l \le N \le l\kappa$, we have $b(N) \equiv 0 \bmod p$.

Next, we treat the case where $l \nmid N$. In this case, $H(p, N/l) = 0$. Then

$$b(N) = \alpha(p)H(p, lN)/p.$$

Assume that $H(p, lN)/p \equiv 0 \bmod p$ for all positive integers N such that

(I) $1 \le N \le l\kappa$,
(II) $l \nmid N$,
(III) $lN \equiv -A \bmod B$,
(IV) $lN \in \mathcal{A}_2$.

Then $b(N) \equiv 0 \bmod p$ for all integers N such that $1 \le N \le l\kappa$. Note that $G_l(z) \in \mathbb{Z}[\![q]\!]$ by Lemma 3.4. Therefore, $\mathrm{ord}_p(G_l(z)) > l\kappa$. Here, we use Theorem 3.3. We see that

$$\begin{aligned}[\varGamma_0(1) : \varGamma_0(lP_2)] &= lP_2 \prod_{q_2 | lP_2,\, q_2 : \text{prime}} (1 + q_2^{-1}) \\ &= l \cdot 4^{m_5} \prod_{r \in \mathfrak{S}_+ \cup \mathfrak{S}_- \cup \{Q\}} r^4 \prod_{r \in \mathfrak{S}_+ \cup \mathfrak{S}_- \cup \{2,l,Q\}} (1 + r^{-1}) \\ &= \frac{3 \cdot 4^{m_5} l(l+1)}{2l} \prod_{r \in \mathfrak{S}_+ \cup \mathfrak{S}_- \cup \{Q\}} r^4 \prod_{r \in \mathfrak{S}_+ \cup \mathfrak{S}_- \cup \{Q\}} \frac{r+1}{r} \\ &= \frac{3 \cdot 4^{m_5}(l+1)}{2} \prod_{r \in \mathfrak{S}_+ \cup \mathfrak{S}_- \cup \{Q\}} r^3(r+1),\end{aligned}$$

where $m_5 := 5$ if $(A, B) = (8, 16)$ and $m_5 := 7$ otherwise. Thus,

$$\begin{aligned}\frac{1}{12}\left(p + \frac{1}{2}\right)[\varGamma_0(1) : \varGamma_0(lP_2)] &= \frac{3 \cdot 4^{m_5}(l+1)(2p+1)}{48} \prod_{r \in \mathfrak{S}_+ \cup \mathfrak{S}_- \cup \{Q\}} r^3(r+1) \\ &= 4^{m_5 - 2}(l+1)(2p+1) \prod_{r \in \mathfrak{S}_+ \cup \mathfrak{S}_- \cup \{Q\}} r^3(r+1) \\ &= (l+1)(\kappa - 1) = l\kappa - l + \kappa - 1.\end{aligned}$$

Since $\kappa < l$, we obtain

$$\frac{1}{12}\left(p + \frac{1}{2}\right)[\varGamma_0(1) : \varGamma_0(lP_2)] < l\kappa.$$

Consequently,

$$\frac{1}{12}\left(p + \frac{1}{2}\right)[\varGamma_0(1) : \varGamma_0(lP_2)] < \mathrm{ord}_p(G_l(z)).$$

Applying Theorem 3.3 to $G_l(z)$, we find that

$$G_l(z) \equiv 0 \bmod p.$$

On the other hand, we will prove that

$$b(-D_0 l^3) \not\equiv 0 \bmod p, \tag{3.2}$$

a contradiction. Indeed,

$$\begin{aligned}
b(-D_0l^3) &= \frac{\alpha(p)}{p}\{H(p,-D_0l^4) - 3H(p,-D_0l^2)\} \\
&= \frac{\alpha(p)H(p,-D_0)}{p}\Big\{\sum_{d\mid l^2}\mu(d)\chi_{D_0}(d)d^{p-1}\sigma_{2p-1}(l^2/d) \\
&\qquad\qquad - 3\sum_{d\mid l}\mu(d)\chi_{D_0}(d)d^{p-1}\sigma_{2p-1}(l/d)\Big\} \\
&= \frac{\alpha(p)H(p,-D_0)}{p}\big\{\sigma_{2p-1}(l^2) + \mu(l)\chi_{D_0}(l)l^{p-1}\sigma_{2p-1}(l) \\
&\qquad\qquad - 3(\sigma_{2p-1}(l) + \mu(l)\chi_{D_0}(l)l^{p-1}\sigma_{2p-1}(1))\big\} \\
&= \frac{\alpha(p)H(p,-D_0)}{p}\big\{1 + l^{2p-1} + l^{2(2p-1)} + l^{p-1}(1 + l^{2p-1}) \\
&\qquad\qquad - 3(1 + l^{2p-1} + l^{p-1})\big\} \\
&\equiv \frac{(3+2-9)\alpha(p)H(p,-D_0)}{p} \equiv \frac{-4\alpha(p)H(p,-D_0)}{p} \equiv 0 \bmod p,
\end{aligned}$$

because $\alpha(p)H(p,-D_0)/p \not\equiv 0 \bmod p$ by the assumption $\lambda_p(\mathbb{Q}(\sqrt{D_0})) = 1$ and Proposition 3.1.

Thus, there exists a positive integer N such that

(I) $1 \le N \le l\kappa$,
(II) $l \nmid N$,
(III) $lN \equiv -A \bmod B$,
(IV) $lN \in \mathcal{A}_2$,
(V) $H(p, lN)/p \not\equiv 0 \bmod p$.

We can take the above N as N_l. The proof of Theorem 3.5 is complete. ∎

Remark 3.6. We need the assumption $D_0 \neq -8$ in the above proof. Since $Q \equiv 1 \bmod 8$, we have

$$\left(\frac{8}{Q}\right) = \left(\frac{2}{Q}\right)^3 = 1 \neq -1.$$

Thus, the coefficient $b(8l^3)$ in $G_l(z)$ is zero. Therefore, if $D_0 = -8$, we cannot use the above discussion.

Using Theorem 3.5, we will prove Theorem 1.8. Let l and N_l be integers as in Theorem 3.5. Then the fundamental discriminant D_l of $\mathbb{Q}(\sqrt{-lN_l})$ satisfies $\lambda_p(\mathbb{Q}(\sqrt{D_l})) = 1$ by Proposition 3.1. Moreover, $D_l \equiv A \bmod B$, $\chi_r(D_l) = 1$ for all $r \in \mathfrak{S}_+$, and $\chi_{r'}(D_l) = -1$ for all $r' \in \mathfrak{S}_-$. Therefore, we can prove Theorem 1.8 by estimating the number of imaginary quadratic fields $\mathbb{Q}(\sqrt{-lN_l})$. First, we check the existence of the prime number l.

Lemma 3.7. *There exist infinitely many prime numbers l satisfying the following conditions:*

(i) $\kappa < l$,

(ii) $l \equiv 1 \bmod P_3$,

(iii) $\chi_D(l) = -1$ *for all* $D \in \mathfrak{S}_p \cup \{D_0\}$.

Proof. We use the Chebotarev density theorem. For convenience, we rewrite $\mathfrak{S}_p = \{D_1, \ldots, D_{n_1}\}$, where n_1 is a positive integer. Set

$$\mathfrak{A} := \mathbb{Q}(\zeta_{P_3}, \sqrt{D_0 D_1}, \ldots, \sqrt{D_0 D_{n_1}}), \qquad \mathfrak{B} := \mathfrak{A}(\sqrt{D_0}).$$

Let $\mathbb{Q}(\zeta_{v_0})$ be a cyclotomic field containing $\mathfrak{B}$.

First, we will show $\sqrt{D_0} \notin \mathfrak{A}$, that is, $[\mathfrak{B} : \mathfrak{A}] = 2$.

(1) We first treat the case where $D \equiv 1 \bmod 8$ (resp. $D \equiv 5 \bmod 8$) for all $D \in \mathfrak{S}_p \cup \{D_0\}$, that is, $(A, B) = (1, 8)$ (resp. $(A, B) = (5, 8)$). Since $r \nmid D_0 D_1 \cdots D_{n_1}$ for all $r \in \mathfrak{S}_+ \cup \mathfrak{S}_- \cup \{2, Q\}$, it is sufficient to show

$$\sqrt{D_0} \notin \mathfrak{C} := \mathbb{Q}(\sqrt{-1}, \sqrt{D_0 D_1}, \ldots, \sqrt{D_0 D_{n_1}}).$$

Suppose $\sqrt{D_0} \in \mathfrak{C}$. We can write

$$D_0 = -\frac{(D_0 D_1)^{\varepsilon_1} \cdots (D_0 D_{n_1})^{\varepsilon_{n_1}}}{\square},$$

where $\varepsilon_i \in \{0, 1\}$ for each $i \in \{1, \ldots, n_1\}$ and $\square$ denotes the square part of $(D_0 D_1)^{\varepsilon_1} \cdots (D_0 D_{n_1})^{\varepsilon_{n_1}}$. Since $D \equiv 1 \bmod 4$ for all $D \in \mathfrak{S}_p \cup \{D_0\}$, and $\square \equiv 1 \bmod 4$, we have

$$-\frac{(D_0 D_1)^{\varepsilon_1} \cdots (D_0 D_{n_1})^{\varepsilon_{n_1}}}{\square} \equiv 3 \bmod 4.$$

On the other hand,

$$D_0 \equiv 1 \bmod 4.$$

This is a contradiction. Thus, $\sqrt{D_0} \notin \mathfrak{C}$, that is, $\sqrt{D_0} \notin \mathfrak{A}$.

(2) We now treat the case where $D \equiv 8 \bmod 16$ for all $D \in \mathfrak{S}_p \cup \{D_0\}$, that is, $(A, B) = (8, 16)$. Since $r \nmid D_0 D_1 \cdots D_{n_1}$ for all $r \in \mathfrak{S}_+ \cup \mathfrak{S}_- \cup \{Q\}$, it is sufficient to show

$$\sqrt{D_0} \notin \mathfrak{D} := \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{D_0 D_1}, \ldots, \sqrt{D_0 D_{n_1}}).$$

Suppose $\sqrt{D_0} \in \mathfrak{D}$. We can write

$$D_0 = -8 \cdot \frac{(D_0 D_1)^{\varepsilon_1} \cdots (D_0 D_{n_1})^{\varepsilon_{n_1}}}{\square},$$

where $\varepsilon_i \in \{0, 1\}$ for each $i \in \{1, \ldots, n_1\}$ and $\square$ denotes the square part of $c_1 := (D_0 D_1)^{\varepsilon_1} \cdots (D_0 D_{n_1})^{\varepsilon_{n_1}}$. Since

$$\left(\frac{D_0 D_i}{Q}\right) = (-1)^2 = 1$$

for all $i \in \{1, \ldots, n_1\}$, and $\left(\frac{-8}{Q}\right) = 1$, we have

$$\left(\frac{-8(c_1/\square)}{Q}\right) = \left(\frac{-8c_1}{Q}\right) = \left(\frac{c_1}{Q}\right) = 1.$$

On the other hand, $\left(\frac{D_0}{Q}\right) = -1$. This is a contradiction. Thus, $\sqrt{D_0} \notin \mathfrak{D}$, that is, $\sqrt{D_0} \notin \mathfrak{A}$.

It follows from $[\mathfrak{B} : \mathfrak{A}] = 2$ that there exists

$$\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_{v_0})/\mathfrak{A}) \setminus \mathrm{Gal}(\mathbb{Q}(\zeta_{v_0})/\mathfrak{B}).$$

We see from the Chebotarev density theorem that there exist infinitely many prime numbers l such that there is a prime ideal $\wp$ of $\mathbb{Q}(\zeta_{v_0})$ over l with $\tau = \left[\frac{\mathbb{Q}(\zeta_{v_0})/\mathbb{Q}}{\wp}\right]$, where $\left[\frac{\mathbb{Q}(\zeta_{v_0})/\mathbb{Q}}{\wp}\right]$ is the Frobenius of $\wp$ in $\mathrm{Gal}(\mathbb{Q}(\zeta_{v_0})/\mathbb{Q})$. Since the number of primes l' such that $l' \leq \kappa$, the number of prime factors of D_0, and the number of prime factors of v_0 are finite, there exist infinitely many prime numbers l with $\kappa < l$ and $l \nmid v_0 D_0$ such that there is a prime ideal $\wp$ of $\mathbb{Q}(\zeta_{v_0})$ over l with $\tau = \left[\frac{\mathbb{Q}(\zeta_{v_0})/\mathbb{Q}}{\wp}\right]$.

Next, we will show that such prime numbers l satisfy conditions (ii) and (iii). Note that each such l is unramified in $\mathbb{Q}(\zeta_{v_0})$, that is, the prime ideal $\wp$ is unramified in $\mathbb{Q}(\zeta_{v_0})$. Then the decomposition group of $\wp$ in $\mathrm{Gal}(\mathbb{Q}(\zeta_{v_0})/\mathbb{Q})$ is $\langle\tau\rangle$. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_{v_0})/\mathfrak{A})$ contains $\langle\tau\rangle$, the subfield of $\mathbb{Q}(\zeta_{v_0})$ corresponding to this decomposition group contains $\mathfrak{A}$. Thus, l splits completely in $\mathfrak{A}$. Since $\mathbb{Q}(\zeta_{P_3})$ is contained in $\mathfrak{A}$, the prime number l splits completely in $\mathbb{Q}(\zeta_{P_3})$. This last property is equivalent to $l \equiv 1 \bmod P_3$ (see [29, Theorem 2.13]). Thus, l satisfies (ii). It follows from $\mathbb{Q}(\sqrt{D_0 D_i}) \subset \mathfrak{A}$ that l splits completely in $\mathbb{Q}(\sqrt{D_0 D_i})$ for all $i \in \{1, \dots, n_1\}$. On the other hand, we see from $\tau \notin \mathrm{Gal}(\mathbb{Q}(\zeta_{v_0})/\mathfrak{B})$ that the prime ideals of $\mathfrak{A}$ over l do not split completely in $\mathfrak{B}$. Thus, l does not split completely in $\mathbb{Q}(\sqrt{D_0})$. We see from $l \nmid D_0$ that l is inert in $\mathbb{Q}(\sqrt{D_0})$. Therefore, we find that $\chi_D(l) = -1$ for all $D \in \mathfrak{S}_p \cup \{D_0\}$, which is (iii). ∎

Next, we estimate the number of imaginary quadratic fields $\mathbb{Q}(\sqrt{-lN_l})$. In Lemma 3.7, we proved that there exist infinitely many prime numbers l satisfying (i) $\kappa < l$, (ii) $l \equiv 1 \bmod P_3$, (iii) $\chi_D(l) = -1$ for all $D \in \mathfrak{S}_p \cup \{D_0\}$. Since the set of prime numbers l satisfying (ii) and (iii) is not empty, we see from the Chinese remainder theorem that there is an arithmetic progression u_1 modulo v_1 with $\gcd(u_1, v_1) = 1$ which contains infinitely many such l. Here, we need the following lemma.

Lemma 3.8. *Let*

$$\mathcal{A}_4 := \{l\text{: an odd prime} \mid l \equiv u_1 \bmod v_1 \text{ and } l > \kappa\},$$

where u_1 and v_1 are the integers mentioned above. Suppose D_l is the fundamental discriminant of $\mathbb{Q}(\sqrt{-lN_l})$, where N_l denotes the integer in Theorem 3.5. *Then, for any fixed $l \in \mathcal{A}_4$, there exists at most one $l' \in \mathcal{A}_4$ such that $D_l = D_{l'}$.*

Proof. For convenience, we rewrite $\mathcal{A}_4 = \{l_i \mid i \in \mathbb{N}\}$. For $l_i, l_j \in \mathcal{A}_4$, we assume that $l_i < l_j$ if i and j are positive integers with $i < j$. Suppose

$D_{l_h} = D_{l_i} = D_{l_j}$, where h, i, and j are positive integers with $h < i < j$. Then

$$-\frac{l_h N_{l_h}}{\square} = -\frac{l_i N_{l_i}}{\square} = -\frac{l_j N_{l_j}}{\square},$$

where $\square$ is the square part of the numerator. By Theorem 3.5,

$$\gcd(l_h, N_{l_h}) = \gcd(l_i, N_{l_i}) = \gcd(l_j, N_{l_j}) = 1.$$

This implies that $l_i l_j \mid N_{l_h}$, so

$$l_i l_j \leq N_{l_h}.$$

On the other hand, Theorem 3.5 shows that $N_{l_h} \leq l_h \kappa$ and $\kappa < l_j$, so

$$N_{l_h} < l_i l_j,$$

a contradiction. ■

From $0 < -D_l \leq l N_l \leq l^2 \kappa$ and Lemma 3.8, we obtain

$$\begin{aligned}
&\sharp\left\{ D \in S_-(X) \;\middle|\; \begin{array}{c} \lambda_p(\mathbb{Q}(\sqrt{D})) = 1, \\ D \equiv A \bmod B, \\ \left(\frac{D}{r}\right) = 1 \text{ for all } r \in \mathfrak{S}_+, \text{ and} \\ \left(\frac{D}{r'}\right) = -1 \text{ for all } r' \in \mathfrak{S}_- \end{array} \right\} \\
&\quad \geq \sharp\left\{ D_l \in S_-(X) \;\middle|\; \begin{array}{c} \mathbb{Q}(\sqrt{D_l}) = \mathbb{Q}(\sqrt{-lN_l}), \\ \text{where } l \in \mathcal{A}_4 \text{ and} \\ N_l \in \mathbb{N} \text{ in Theorem 3.5} \end{array} \right\} \\
&\quad \geq \tfrac{1}{2}\sharp\{ l \in \mathcal{A}_4 \mid 0 \leq l^2\kappa \leq X \} \\
&\quad = \tfrac{1}{2}\sharp\{ l\text{: an odd prime} \mid l \equiv u_1 \bmod v_1,\ l > \kappa, \text{ and } l^2\kappa \leq X \} \\
&\quad = \tfrac{1}{2}\sharp\{ l\text{: an odd prime} \mid l \equiv u_1 \bmod v_1 \text{ and } 0 < l \leq \sqrt{X}/\sqrt{\kappa} \} \\
&\qquad - \tfrac{1}{2}\sharp\{ l\text{: an odd prime} \mid l \equiv u_1 \bmod v_1 \text{ and } 0 < l \leq \kappa \}
\end{aligned}$$

for any sufficiently large $X \in \mathbb{R}$. Let

$$E(X) := \tfrac{1}{2}\sharp\{ l\text{: an odd prime} \mid l \equiv u_1 \bmod v_1 \text{ and } 0 < l \leq \sqrt{X}/\sqrt{\kappa} \}.$$

By the Dirichlet theorem on primes in arithmetic progression, we have

$$E(X) \sim \frac{\sqrt{X}}{\varphi(v_1)\sqrt{\kappa}(\log X - \log \kappa)}$$

for any sufficiently large $X \in \mathbb{R}$. Then, under the assumption of the existence of D_0, we see that

$$\sharp\left\{D \in S_-(X) \;\middle|\; \begin{array}{c} \lambda_p(\mathbb{Q}(\sqrt{D})) = 1, \\ D \equiv A \bmod B, \\ \left(\frac{D}{r}\right) = 1 \text{ for all } r \in \mathfrak{S}_+, \text{ and} \\ \left(\frac{D}{r'}\right) = -1 \text{ for all } r' \in \mathfrak{S}_- \end{array}\right\} \gg \frac{\sqrt{X}}{\log X}$$

for any sufficiently large $X \in \mathbb{R}$. The proof of Theorem 1.8 is complete.

4. Proofs of Theorems 1.11 and 1.14. First, we outline the proofs. We will prove the following two theorems.

THEOREM 4.1. *Let p be an odd prime number, n an integer greater than* 1 *such that* $\gcd(p, n) = 1$, *and x_1 a positive integer such that* $\gcd(x_1, p) = 1$.

(1) *Assume that $x_1^2 < p^n$. Then $\lambda_p(\mathbb{Q}(\sqrt{x_1^2 - p^n})) = 1$ if and only if $p \nmid h(\mathbb{Q}(\sqrt{x_1^2 - p^n}))$ and $(2x_1)^{p-1} \not\equiv 1 \bmod p^2$.*

(2) *Assume that $x_1^2 < 4p^n$ and x_1 is odd. Then $\lambda_p(\mathbb{Q}(\sqrt{x_1^2 - 4p^n})) = 1$ if and only if $p \nmid h(\mathbb{Q}(\sqrt{x_1^2 - 4p^n}))$ and $x_1^{p-1} \not\equiv 1 \bmod p^2$.*

Applying Theorem 4.1(1) to $x_1 = 1, 2, q_1, 2q_1$, we obtain the imaginary quadratic fields in Theorem 1.11. Let us give some additional explanation for $x_1 = 2$. Note that $2^{p-1} \not\equiv -1 \bmod p^2$, since otherwise $2^{p-1} + 1 \equiv 0 \bmod p$ and $2^{p-1} - 1 \equiv 0 \bmod p$, contradicting $\gcd(2^{p-1}+1, 2^{p-1}-1) = 1$. Therefore, since $2^{p-1} \not\equiv 1 \bmod p^2$, also $2^{2(p-1)} \not\equiv 1 \bmod p^2$. Thus, using Theorem 4.1(1) for $x_1 = 2$, we find that if $p \nmid h(\mathbb{Q}(\sqrt{4 - p^n}))$ and $2^{p-1} \not\equiv 1 \bmod p^2$, then $\lambda_p(\mathbb{Q}(\sqrt{4 - p^n})) = 1$. We also obtain the imaginary quadratic fields treated in Theorem 1.14 by applying Theorem 4.1(2) to $x_1 = 1$.

THEOREM 4.2. *Let p be an odd prime number, q_1 a prime factor of $p - 2$ such that $q_1^{p-1} \not\equiv 1 \bmod p^2$, and n an integer greater than* 1.

(1) *Assume $p \equiv 3 \bmod 4$.*

  (i) *Suppose $p = 3$. If n is an odd integer such that $n \neq 5$, then the order of the ideal class containing the prime ideal of $\mathbb{Q}(\sqrt{1 - p^n})$ over p is n. When $n = 5$, we see that $\mathbb{Q}(\sqrt{1 - 3^5}) = \mathbb{Q}(\sqrt{-2})$. The class number of $\mathbb{Q}(\sqrt{-2})$ is 1, and the order of the ideal class containing the prime ideal of $\mathbb{Q}(\sqrt{-2})$ over 3 is 1.*

  (ii) *Suppose $p \neq 3$. If n is an odd integer, then the order of the ideal class containing the prime ideal of $\mathbb{Q}(\sqrt{1 - p^n})$ over p is n.*

  (iii) *Suppose $2^{p-1} \equiv 1 \bmod p^2$. If n is an odd composite number, then the order of the ideal class containing the prime ideal of $\mathbb{Q}(\sqrt{q_1^2 - p^n})$ over p is n.*

(2) *Assume* $p \equiv 1 \bmod 4$.

(i) *Suppose* $\mathbb{Q}(\sqrt{4-p^n}) \neq \mathbb{Q}(\sqrt{-1})$. *Then the order of the ideal class containing the prime ideal of* $\mathbb{Q}(\sqrt{4-p^n})$ *over* p *is* n (*see* [15, Theorem 1(2)]).

(ii) *Suppose* $2^{p-1} \equiv 1 \bmod p^2$, $4q_1^2 < p^n$, *and* $\mathbb{Q}(\sqrt{4q_1^2-p^n}) \neq \mathbb{Q}(\sqrt{-1})$. *If* n *is a composite number, then the order of the ideal class containing the prime ideal of* $\mathbb{Q}(\sqrt{4q_1^2-p^n})$ *over* p *is* n.

(3) *If* $n > 8$, *then the order of the ideal class containing the prime ideal of* $\mathbb{Q}(\sqrt{1-4p^n})$ *over* p *is* n (*see* [14, Theorem] *or* [16]).

Combining Theorems 4.1(1) and 4.2(1), (2), we get Theorem 1.11. Similarly, we obtain Theorem 1.14 by using Theorems 4.1(2) and 4.2(3). Theorems 4.1 and 4.2 will be shown in the next two subsections.

4.1. Proof of Theorem 4.1. The method of proof is the same as in Section 2. We mainly use Theorem 2.1.

First, we analyse $\mathbb{Q}(\sqrt{x_1^2-p^n})$. We can write

$$(p)^n = \big(x_1 + \sqrt{x_1^2-p^n}\big)\big(x_1 - \sqrt{x_1^2-p^n}\big)$$

in $\mathbb{Q}(\sqrt{x_1^2-p^n})$. Set $\alpha := x_1+\sqrt{x_1^2-p^n}$. Since $\gcd(p, x_1^2-p^n) = 1$ and $p \nmid \alpha$, p splits in $\mathbb{Q}(\sqrt{x_1^2-p^n})$. Note that the ideals (α) and $(\overline{\alpha})$ are coprime, where $\overline{\alpha}$ is the complex conjugate of α. Thus,

$$(\alpha) = \wp^n,$$

where $\wp$ is the prime ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{x_1^2-p^n})}$ over p. Applying Theorem 2.1 for $m_1 = n$ and $\xi = \alpha$, we find that $\lambda_p(\mathbb{Q}(\sqrt{x_1^2-p^n})) = 1$ if and only if $p \nmid h(\mathbb{Q}(\sqrt{x_1^2-p^n}))$ and

$$\big(x_1 + \sqrt{x_1^2-p^n}\big)^{p-1} - 1 \not\equiv 0 \bmod \overline{\wp}^2, \tag{4.1}$$

where $\overline{\wp}$ is the complex conjugate of $\wp$. Condition (4.1) is equivalent to

$$\big(x_1 + \sqrt{x_1^2-p^n}\big)^{p} - \big(x_1 + \sqrt{x_1^2-p^n}\big) \not\equiv 0 \bmod \overline{\wp}^2\wp^n. \tag{4.2}$$

We see that

$$\begin{aligned}\big(x_1 &+ \sqrt{x_1^2-p^n}\big)^{p} - \big(x_1 + \sqrt{x_1^2-p^n}\big)\\ &= \bigg\{\sum_{j=0}^{p}\binom{p}{j}x_1^{p-j}\big(\sqrt{x_1^2-p^n}\big)^j\bigg\} - \big(x_1 + \sqrt{x_1^2-p^n}\big)\end{aligned}$$

$$
\begin{aligned}
&= \Bigg\{ \sum_{j=0}^{(p-1)/2} \binom{p}{2j} x_1^{p-2j}(x_1^2-p^n)^j \Bigg\} \\
&\quad + \Bigg\{ \sum_{j=0}^{(p-1)/2} \binom{p}{2j+1} x_1^{p-2j-1}(x_1^2-p^n)^j \sqrt{x_1^2-p^n} \Bigg\} - x_1 - \sqrt{x_1^2-p^n}.
\end{aligned}
$$

When $n \geq 2$, we have $p^n \equiv 0 \bmod \overline{\wp}^2\wp^n$. Thus,

$$
\begin{aligned}
&\big(x_1+\sqrt{x_1^2-p^n}\big)^p - \big(x_1+\sqrt{x_1^2-p^n}\big) \\
&\equiv \Bigg\{ \sum_{j=0}^{(p-1)/2} \binom{p}{2j} x_1^{p-2j} x_1^{2j} \Bigg\} + \Bigg\{ \sum_{j=0}^{(p-1)/2} \binom{p}{2j+1} x_1^{p-2j-1} x_1^{2j} \sqrt{x_1^2-p^n} \Bigg\} \\
&\qquad - x_1 - \sqrt{x_1^2-p^n} \\
&\equiv x_1^p \Bigg\{ \sum_{j=0}^{(p-1)/2} \binom{p}{2j} \Bigg\} + x_1^{p-1}\sqrt{x_1^2-p^n} \Bigg\{ \sum_{j=0}^{(p-1)/2} \binom{p}{2j+1} \Bigg\} - x_1 - \sqrt{x_1^2-p^n} \\
&\equiv 2^{p-1}x_1^p + 2^{p-1}x_1^{p-1}\sqrt{x_1^2-p^n} - x_1 - \sqrt{x_1^2-p^n} \\
&\equiv \big(x_1+\sqrt{x_1^2-p^n}\big)(2^{p-1}x_1^{p-1}-1) \bmod \overline{\wp}^2\wp^n.
\end{aligned}
$$

Consequently, (4.2) is true if and only if

$$(2x_1)^{p-1} - 1 \not\equiv 0 \bmod p^2.$$

Therefore, $\lambda_p(\mathbb{Q}(\sqrt{x_1^2-p^n})) = 1$ if and only if $p \nmid h(\mathbb{Q}(\sqrt{x_1^2-p^n}))$ and $(2x_1)^{p-1} \not\equiv 1 \bmod p^2$, proving (1).

Next, we analyse $\mathbb{Q}(\sqrt{x_1^2-4p^n})$. We can write

$$(p)^n = \left(\frac{x_1+\sqrt{x_1^2-4p^n}}{2}\right)\left(\frac{x_1-\sqrt{x_1^2-4p^n}}{2}\right)$$

in $\mathbb{Q}(\sqrt{x_1^2-4p^n})$. Set $\beta := (x_1+\sqrt{x_1^2-4p^n})/2$. Since $\gcd(p, x_1^2-4p^n) = 1$ and $p \nmid \beta$, p splits in $\mathbb{Q}(\sqrt{x_1^2-4p^n})$. Since the ideals (β) and $(\overline{\beta})$ are coprime, we have

$$(\beta) = \wp^n,$$

where $\wp$ is the prime ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{x_1^2-4p^n})}$ over p. Applying Theorem 2.1 for $m_1 = n$ and $\xi = \beta$, we find that $\lambda_p(\mathbb{Q}(\sqrt{x_1^2-4p^n})) = 1$ if and only if $p \nmid h(\mathbb{Q}(\sqrt{x_1^2-4p^n}))$ and

$$\left(\frac{x_1+\sqrt{x_1^2-4p^n}}{2}\right)^{p-1} - 1 \not\equiv 0 \bmod \overline{\wp}^2, \tag{4.3}$$

where $\overline{\wp}$ is the complex conjugate of $\wp$. Condition (4.3) is equivalent to

$$\left(\frac{x_1+\sqrt{x_1^2-4p^n}}{2}\right)^p-\frac{x_1+\sqrt{x_1^2-4p^n}}{2}\not\equiv 0 \bmod \overline{\wp}^2\wp^n. \tag{4.4}$$

We see that

$$\begin{aligned}
&\left(\frac{x_1+\sqrt{x_1^2-4p^n}}{2}\right)^p-\frac{x_1+\sqrt{x_1^2-4p^n}}{2}\\
&\quad=\frac{1}{2^p}\big(x_1+\sqrt{x_1^2-4p^n}\big)^p-\frac{1}{2}\big(x_1+\sqrt{x_1^2-4p^n}\big)\\
&\quad=\frac{1}{2^p}\left\{\sum_{j=0}^{p}\binom{p}{j}x_1^{p-j}\big(\sqrt{x_1^2-4p^n}\big)^j\right\}-\frac{1}{2}\big(x_1+\sqrt{x_1^2-4p^n}\big)\\
&\quad=\frac{1}{2^p}\left\{\sum_{j=0}^{(p-1)/2}\binom{p}{2j}x_1^{p-2j}(x_1^2-4p^n)^j\right.\\
&\qquad\left.+\sum_{j=0}^{(p-1)/2}\binom{p}{2j+1}x_1^{p-2j-1}(x_1^2-4p^n)^j\sqrt{x_1^2-4p^n}\right\}-\frac{1}{2}\big(x_1+\sqrt{x_1^2-4p^n}\big).
\end{aligned}$$

When $n\ge 2$, we have $p^n\equiv 0 \bmod \overline{\wp}^2\wp^n$. Thus,

$$\begin{aligned}
&\left(\frac{x_1+\sqrt{x_1^2-4p^n}}{2}\right)^p-\frac{x_1+\sqrt{x_1^2-4p^n}}{2}\\
&\equiv\frac{1}{2^p}\left\{\sum_{j=0}^{(p-1)/2}\binom{p}{2j}x_1^{p-2j}x_1^{2j}+\sum_{j=0}^{(p-1)/2}\binom{p}{2j+1}x_1^{p-2j-1}x_1^{2j}\sqrt{x_1^2-4p^n}\right\}\\
&\quad-\frac{1}{2}\big(x_1+\sqrt{x_1^2-4p^n}\big)\\
&\equiv\frac{1}{2^p}\left\{x_1^p\sum_{j=0}^{(p-1)/2}\binom{p}{2j}+x_1^{p-1}\sqrt{x_1^2-4p^n}\sum_{j=0}^{(p-1)/2}\binom{p}{2j+1}\right\}-\frac{1}{2}\big(x_1+\sqrt{x_1^2-4p^n}\big)\\
&\equiv\frac{1}{2^p}\big(2^{p-1}x_1^p+2^{p-1}x_1^{p-1}\sqrt{x_1^2-4p^n}\big)-\frac{1}{2}\big(x_1+\sqrt{x_1^2-4p^n}\big)\\
&\equiv\frac{1}{2}\big(x_1^p+x_1^{p-1}\sqrt{x_1^2-4p^n}\big)-\frac{1}{2}\big(x_1+\sqrt{x_1^2-4p^n}\big)\\
&\equiv\frac{1}{2}\big(x_1+\sqrt{x_1^2-4p^n}\big)(x_1^{p-1}-1) \bmod \overline{\wp}^2\wp^n.
\end{aligned}$$

Consequently, (4.4) is true if and only if

$$x_1^{p-1}-1\not\equiv 0 \bmod p^2.$$

Therefore, $\lambda_p(\mathbb{Q}(\sqrt{x_1^2-4p^n}))=1$ if and only if $p\nmid h(\mathbb{Q}(\sqrt{x_1^2-4p^n}))$ and $x_1^{p-1}\not\equiv 1 \bmod p^2$, proving (2). ∎

4.2. Proof of Theorem 4.2. In this section, we show Theorem 4.2(1) and (2)(ii). Clauses (2)(i) and (3) are already proved (see [14]–[16]). First, we outline the proof. The method of proof is based on [20] and [15].

Let p be an odd prime number and n a positive integer satisfying the assumption in Theorem 4.2(1) and (2)(ii). We analyse the imaginary quadratic field $\mathbb{Q}(\sqrt{x_1^2-p^n})$, where $x_1 = 1$, q_1, $2q_1$. We can write

$$(p)^n = \big(x_1+\sqrt{x_1^2-p^n}\big)\big(x_1-\sqrt{x_1^2-p^n}\big)$$

in $\mathbb{Q}(\sqrt{x_1^2-p^n})$. Set $\alpha := x_1+\sqrt{x_1^2-p^n}$. Since $\gcd(p, x_1^2-p^n) = 1$ and $p \nmid \alpha$, the prime number p splits in $\mathbb{Q}(\sqrt{x_1^2-p^n})$. The ideals (α) and $(\overline{\alpha})$ are coprime, so

$$(\alpha) = \wp^n,$$

where $\wp$ is the prime ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{x_1^2-p^n})}$ over p. We will prove that the order of the ideal class containing $\wp$ is n. It is essential for this proof to show that $\pm\alpha$ is not a p_4th power in $\mathcal{O}_{\mathbb{Q}(\sqrt{x_1^2-p^n})}$ for any prime number p_4 dividing n. We prove this by checking that there is no integer solution (u, v) of the equation

$$\pm\alpha = (u+v\sqrt{d_0})^{p_4},$$

where d_0 is the square-free part of $x_1^2-p^n$.

In Section 4.2.1, we prove Theorem 4.2(1)(i) and (ii). In Section 4.2.2, we show Theorem 4.2(1)(iii). In Section 4.2.3, we prove Theorem 4.2(2)(ii).

4.2.1. *Proof of Theorem 4.2(1)(i) and (ii).* First, we prepare the following lemma:

LEMMA 4.3. *Let p be an odd prime number. Then, for any given positive even integer d_1, the equation*

$$d_1x^2+1 = p^y$$

has at most one positive integer solution (x, y) except for $(d_1, p) = (2, 3)$ when the solutions are $(x, y) = (1, 1)$, $(2, 2)$, $(11, 5)$.

We prove this by using a result of Y. Bugeaud and T. N. Shorey [1] which we now state.

Let $\mathcal{F}_n$ denote the nth Fibonacci number defined by $\mathcal{F}_0 := 0$, $\mathcal{F}_1 := 1$, and $\mathcal{F}_{n+2} := \mathcal{F}_{n+1}+\mathcal{F}_n$ for all $n \geq 0$. Let $\mathcal{L}_n$ denote the nth Lucas number defined by $\mathcal{L}_0 := 2$, $\mathcal{L}_1 := 1$, and $\mathcal{L}_{n+2} := \mathcal{L}_{n+1}+\mathcal{L}_n$ for all $n \geq 0$. We define $\mathfrak{F}, \mathfrak{G} \subset \mathbb{N}\times\mathbb{N}\times\mathbb{N}$ by

$$\mathfrak{F} := \{(\mathcal{F}_{h-2\varepsilon}, \mathcal{L}_{h+\varepsilon}, \mathcal{F}_h) \mid h \in \mathbb{N} \text{ such that } h \geq 2 \text{ and } \varepsilon \in \{\pm 1\}\},$$

$$\mathfrak{G} := \{(1, 4p_5^{h_1}-1, p_5) \mid p_5 \text{ is a prime number and } h_1 \in \mathbb{N}\}.$$

Bugeaud and Shorey gave the following result.

Theorem 4.4 (Bugeaud and Shorey, [1, Theorem 1]). *Let p be a prime number, and d_1 and d_2 coprime positive integers such that* $\gcd(d_1d_2, p) = 1$. *Let $\gamma \in \{1, \sqrt{2}, 2\}$ be such that $\gamma = 2$ if $p = 2$. Assume that d_2 is odd if $\gamma \in \{\sqrt{2}, 2\}$. Then the equation*

$$d_1x^2 + d_2 = \gamma^2p^y$$

has at most one positive integer solution (x, y) except for

$$(\gamma, d_1, d_2, p) \in \mathfrak{E} := \left\{ \begin{matrix} (2, 13, 3, 2), (\sqrt{2}, 7, 11, 3), (1, 2, 1, 3), (2, 7, 1, 2), \\ (\sqrt{2}, 1, 1, 5), (\sqrt{2}, 1, 1, 13), (2, 1, 3, 7) \end{matrix} \right\}$$

or

$$(d_1, d_2, p) \in \mathfrak{F} \cup \mathfrak{G} \cup \mathfrak{H}_\gamma,$$

where $\mathfrak{H}_\gamma$ denotes the set

$$\mathfrak{H}_\gamma := \left\{ (d_1, d_2, p) \;\middle|\; \begin{matrix} \textit{there exist positive integers } s_0 \textit{ and } t_0 \\ \textit{such that } d_1s_0^2 + d_2 = \gamma^2p^{t_0} \textit{ and} \\ 3d_1s_0^2 - d_2 = \pm\gamma^2 \end{matrix} \right\}.$$

This theorem is also used in Sections 4.2.2 and 4.2.3.

Proof of Lemma 4.3. We will show

$$(\gamma, d_1, d_2, p) = (1, d_1, 1, p) \notin \mathfrak{E} \setminus \{(1, 2, 1, 3)\}$$

and

$$(d_1, d_2, p) = (d_1, 1, p) \notin \mathfrak{F} \cup \mathfrak{G} \cup \mathfrak{H}_1$$

in order to use Theorem 4.4 with $\gamma = 1$.

We easily see that $(1, d_1, 1, p) \notin \mathfrak{E} \setminus \{(1, 2, 1, 3)\}$ and $(d_1, 1, p) \notin \mathfrak{G}$. Suppose $(d_1, 1, p) \in \mathfrak{F}$. There exists an integer $h > 1$ such that $\mathcal{F}_{h-2\varepsilon} = d_1$, $\mathcal{L}_{h+\varepsilon} = 1$, and $\mathcal{F}_h = p$, where $\varepsilon = \pm 1$. The integer h must be 0 or 2 since $\mathcal{L}_{h+\varepsilon} = 1$. Since $h > 1$, it must be 2. When $h = 2$, the 2nd Fibonacci number $\mathcal{F}_2$ is 1. This is a contradiction. Thus, $(d_1, 1, p) \notin \mathfrak{F}$. Next suppose $(d_1, 1, p) \in \mathfrak{H}_1$. Then $d_1s_0^2 + 1 = p^{t_0}$ and $3d_1s_0^2 - 1 = \pm 1$ for some positive integers s_0 and t_0. Then $4 = 3p^{t_0} \pm 1$, that is, $3p^{t_0} = 3$ or 5, a contradiction. Therefore, $(d_1, 1, p) \notin \mathfrak{H}_1$.

When $(d_1, p) = (2, 3)$, the statement of this lemma follows from [23, Theorem 2.3]. ■

Next, we prove the following key lemma by using Lemma 4.3.

Lemma 4.5. *Let p be a prime number such that $p \equiv 3 \bmod 4$, n an odd integer greater than 1 such that $(p, n) \neq (3, 5)$, and*

$$\alpha := 1 + \sqrt{1 - p^n}.$$

Then $\pm\alpha$ is not a p_4th power in $\mathcal{O}_{\mathbb{Q}(\sqrt{1-p^n})}$ for any prime p_4 dividing n.

Proof. Since p_4 is odd, it is sufficient to prove that α is not a p_4th power in $\mathcal{O}_{\mathbb{Q}(\sqrt{1-p^n})}$. We see from $p \equiv 3 \bmod 4$ and $n \equiv 1 \bmod 2$ that $1 - p^n \equiv 2 \bmod 4$. Then $\mathcal{O}_{\mathbb{Q}(\sqrt{1-p^n})} = \mathbb{Z}[\sqrt{d_0}]$, where d_0 is the square-free part of $1 - p^n$.

Suppose α is a p_4th power in $\mathcal{O}_{\mathbb{Q}(\sqrt{1-p^n})}$. Write

$$\alpha = (u + v\sqrt{d_0})^{p_4} \tag{4.5}$$

for some integers u and v. Expanding the right side, we have

$$1 + \sqrt{1-p^n} = \left\{ \sum_{j=0}^{(p_4-1)/2} \binom{p_4}{2j} u^{p_4-2j}(v^2 d_0)^j \right\} + w\sqrt{d_0}$$

for some integer w. Equating the real parts gives

$$1 = u \sum_{j=0}^{(p_4-1)/2} \binom{p_4}{2j} u^{p_4-2j-1}(v^2 d_0)^j.$$

This implies that $u = \pm 1$. Hence,

$$1 + \sqrt{1-p^n} = \left(\pm 1 + v\sqrt{d_0} \right)^{p_4}.$$

Taking the norm of this, we obtain $p^n = (1 - v^2 d_0)^{p_4}$. Then

$$p^{n/p_4} = 1 - v^2 d_0.$$

On the other hand, we can write

$$1 - p^n = c^2 d_0$$

for some positive integer c. These imply that both $(x, y) = (c, n)$ and $(x, y) = (|v|, n/p_4)$ are positive integer solutions of $-d_0 x^2 + 1 = p^y$. This is a contradiction when $(-d_0, p) \neq (2, 3)$ by Lemma 4.3. If $(-d_0, p) = (2, 3)$, it follows from Lemma 4.3 that $(c, n) = (1, 1)$, $(2, 2)$, $(11, 5)$. Since n is an odd integer greater than 1, the pair (c, n) must be $(11, 5)$. But the case where $(p, n) = (3, 5)$ is excluded in this lemma. ∎

Finally, we show Theorem 4.2(1)(i) and (ii) by using Lemma 4.5.

Proof of Theorem 4.2(1)(i) and (ii). Since $\gcd(p, 1 - p^n) = 1$ and $p \nmid \alpha$, the prime number p splits in $\mathbb{Q}(\sqrt{1-p^n})$. The ideals (α) and $(\overline{\alpha})$ are coprime, so

$$(\alpha) = \wp^n,$$

where $\wp$ is the prime ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{1-p^n})}$ over p. Let s_1 be the order of the ideal class containing $\wp$. We can write $n = s_1 t_1$ for some integer t_1. Since $\wp^{s_1}$ is principal, there exists $\eta \in \mathcal{O}_{\mathbb{Q}(\sqrt{1-p^n})}$ such that $\wp^{s_1} = (\eta)$. Then

$$(\alpha) = (\wp^{s_1})^{t_1} = (\eta)^{t_1} = (\eta^{t_1}).$$

Since $\mathbb{Q}(\sqrt{1-p^n}) \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, this implies that

$$\pm\alpha = \eta^{t_1}.$$

When $(p,n) \neq (3,5)$, we obtain $t_1 = 1$ by Lemma 4.5. Thus, $s_1 = n$ when $(p,n) \neq (3,5)$. ■

4.2.2. *Proof of Theorem 4.2(1)(iii).* The method of proof is basically similar to the one in Section 4.2.1. First, we prepare two lemmas.

LEMMA 4.6. *Let p and q_5 be distinct odd prime numbers. Then the equation*

$$4q_5^2 - 3p^x = \pm 1$$

has no positive integer solution x.

Proof. Suppose x is such solution. If $q_5 = 3$, we have

$$4q_5^2 - 3p^x \equiv 0 \bmod 3,$$

a contradiction. Therefore, $q_5 \neq 3$. First, we treat the equation $4q_5^2 - 3p^x = -1$. Since $q_5^2 \equiv 1 \bmod 3$, we have

$$4q_5^2 - 3p^x \equiv 4 - 0 \equiv 1 \bmod 3,$$

a contradiction. Next, we treat the equation $4q_5^2 - 3p^x = 1$. We can write

$$3p^x = 4q_5^2 - 1 = (2q_5+1)(2q_5-1).$$

Since $\gcd(2q_5+1, 2q_5-1) = 1$, we obtain four cases: (i) $2q_5+1 = p^x$, $2q_5 - 1 = 3$, (ii) $2q_5+1 = 3$, $2q_5-1 = p^x$, (iii) $2q_5+1 = 3p^x$, $2q_5-1 = 1$, (iv) $2q_5+1 = 1$, $2q_5-1 = 3p^x$. We easily see that the above four cases are all impossible. ■

We use this to show the following lemma.

LEMMA 4.7. *Let p and q_5 be distinct odd prime numbers. Then, for any given positive even integer d_1, the equation*

$$d_1x^2 + q_5^2 = p^y$$

has at most one positive integer solution (x,y).

Proof. We will show

$$(\gamma, d_1, d_2, p) = (1, d_1, q_5^2, p) \notin \mathfrak{E}$$

and

$$(d_1, d_2, p) = (d_1, q_5^2, p) \notin \mathfrak{F} \cup \mathfrak{G} \cup \mathfrak{H}_1$$

in order to use Theorem 4.4 with $\gamma = 1$.

We easily see that $(1, d_1, q_5^2, p) \notin \mathfrak{E}$ and $(d_1, q_5^2, p) \notin \mathfrak{G}$. Suppose $(d_1, q_5^2, p) \in \mathfrak{F}$. There is an integer $h > 1$ such that $\mathcal{F}_{h-2\varepsilon} = d_1$, $\mathcal{L}_{h+\varepsilon} = q_5^2$, and $\mathcal{F}_h = p$, where $\varepsilon = \pm 1$. J. H. E. Cohn [9] proved that $\mathcal{L}_1 = 1$ and $\mathcal{L}_3 = 4$ are the only squares in the Lucas sequence. Thus, $\mathcal{L}_{h+\varepsilon} = q_5^2$ is impossible. Therefore,

$(d_1, q_5^2, p) \notin \mathfrak{F}$. Next suppose $(d_1, q_5^2, p) \in \mathfrak{H}_1$. Then $d_1 s_0^2 + q_5^2 = p^{t_0}$ and $3d_1 s_0^2 - q_5^2 = \pm 1$ for some positive integers s_0 and t_0. Hence, $4q_5^2 = 3p^{t_0} \pm 1$, contrary to Lemma 4.6. Therefore, $(d_1, q_5^2, p) \notin \mathfrak{H}_1$. ■

LEMMA 4.8. *Let p be a prime number such that $p \equiv 3 \bmod 4$ and $2^{p-1} \equiv 1 \bmod p^2$, q_1 a prime factor of $p-2$ such that $q_1^{p-1} \not\equiv 1 \bmod p^2$, n an odd composite number, and*

$$\alpha := q_1 + \sqrt{q_1^2 - p^n}.$$

Then $\pm\alpha$ is not a p_4th power in $\mathcal{O}_{\mathbb{Q}(\sqrt{q_1^2-p^n})}$ for any prime p_4 dividing n.

Proof. Since p_4 is odd, it is sufficient to prove that α is not a p_4th power in $\mathcal{O}_{\mathbb{Q}(\sqrt{q_1^2-p^n})}$. Suppose α is a p_4th power in $\mathcal{O}_{\mathbb{Q}(\sqrt{q_1^2-p^n})}$. It follows from the assumptions $p \equiv 3 \bmod 4$, $q_1 \equiv 1 \bmod 2$, and $n \equiv 1 \bmod 2$ that $q_1^2 - p^n \equiv 2 \bmod 4$. Then $\mathcal{O}_{\mathbb{Q}(\sqrt{q_1^2-p^n})} = \mathbb{Z}[\sqrt{d_0}]$, where d_0 is the square-free part of $q_1^2 - p^n$.

Suppose that

$$\alpha = (u + v\sqrt{d_0})^{p_4} \tag{4.6}$$

for some integers u and v. Expanding the right side, we get

$$q_1 + \sqrt{q_1^2 - p^n} = \left\{ \sum_{j=0}^{(p_4-1)/2} \binom{p_4}{2j} u^{p_4-2j} (v^2 d_0)^j \right\} + w\sqrt{d_0}$$

for some integer w. Equating the real parts gives

$$q_1 = u \sum_{j=0}^{(p_4-1)/2} \binom{p_4}{2j} u^{p_4-2j-1} (v^2 d_0)^j. \tag{4.7}$$

This implies that $u = \pm 1$ or $\pm q_1$. Suppose $u = \pm q_1$. Then

$$q_1 + \sqrt{q_1^2 - p^n} = \big(\pm q_1 + v\sqrt{d_0}\big)^{p_4}.$$

Taking the norm of this, we obtain $p^n = (q_1^2 - v^2 d_0)^{p_4}$. Hence,

$$p^{n/p_4} = q_1^2 - v^2 d_0.$$

On the other hand, we can write

$$q_1^2 - p^n = c^2 d_0$$

for some positive integer c. These imply that both $(x, y) = (c, n)$ and $(x, y) = (|v|, n/p_4)$ are positive integer solutions of $-d_0 x^2 + q_1^2 = p^y$, contradicting Lemma 4.7. Thus, u must be ± 1. Substituting $u = \pm 1$ in equation (4.7), we obtain

$$\pm q_1 = \sum_{j=0}^{(p_4-1)/2} \binom{p_4}{2j} (v^2 d_0)^j. \tag{4.8}$$

Taking the norm of $\alpha = (\pm 1 + v\sqrt{d_0})^{p_4}$, we have $p^n = (1 - v^2 d_0)^{p_4}$. Hence, $p^{n/p_4} = 1 - v^2 d_0$, that is, $v^2 d_0 = 1 - p^{n/p_4}$. Substituting this in (4.8), we obtain

$$\pm q_1 = \sum_{j=0}^{(p_4-1)/2} \binom{p_4}{2j} (1 - p^{n/p_4})^j.$$

Since n is a composite number, we have $n/p_4 \geq 2$. Then $p^{n/p_4} \equiv 0 \bmod p^2$. Using this, we see that

$$\pm q_1 = \sum_{j=0}^{(p_4-1)/2} \binom{p_4}{2j} (1 - p^{n/p_4})^j \equiv \sum_{j=0}^{(p_4-1)/2} \binom{p_4}{2j} \equiv 2^{p_4 - 1} \bmod p^2.$$

Combining this and the assumption $2^{p-1} \equiv 1 \bmod p^2$, we obtain

$$q_1^{p-1} \equiv (\pm q_1)^{p-1} \equiv (2^{p_4-1})^{p-1} \equiv (2^{p-1})^{p_4-1} \equiv 1 \bmod p^2,$$

a contradiction. ∎

Finally, we show Theorem 4.2(1)(iii) by using Lemma 4.8.

Proof of Theorem 4.2(1)(iii). Since $\gcd(p, q_1^2 - p^n) = 1$ and $p \nmid \alpha$, the prime number p splits in $\mathbb{Q}(\sqrt{q_1^2 - p^n})$. Since the ideals (α) and $(\overline{\alpha})$ are coprime, we have

$$(\alpha) = \wp^n,$$

where $\wp$ is the prime ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{q_1^2 - p^n})}$ over p. Let s_1 be the order of the ideal class containing $\wp$. We can write $n = s_1 t_1$ for some integer t_1. Since $\wp^{s_1}$ is principal, there exists $\eta \in \mathcal{O}_{\mathbb{Q}(\sqrt{q_1^2 - p^n})}$ such that $\wp^{s_1} = (\eta)$. Then

$$(\alpha) = (\wp^{s_1})^{t_1} = (\eta)^{t_1} = (\eta^{t_1}).$$

Since $\mathbb{Q}(\sqrt{q_1^2 - p^n}) \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, this implies that $\pm\alpha = \eta^{t_1}$. We obtain $t_1 = 1$ by Lemma 4.8, so $s_1 = n$. ∎

4.2.3. *Proof of Theorem 4.2(2)(ii).* The method of proof is also similar to the one in Section 4.2.1. First, we prepare two lemmas.

Lemma 4.9. *Let p and q_6 be distinct odd prime numbers. Then the equation*

$$16 q_6^2 - 3p^x = \pm 1$$

has no positive integer solution x.

Proof. Suppose x is such a solution. If $q_6 = 3$, we have

$$16 q_6^2 - 3p^x \equiv 0 \bmod 3,$$

a contradiction. Therefore, $q_6 \neq 3$. First, we treat the equation $16q_6^2 - 3p^x = -1$. Since $q_6^2 \equiv 1 \bmod 3$, we have

$$16 q_6^2 - 3p^x \equiv 1 - 0 \equiv 1 \bmod 3,$$

a contradiction. Next, we treat the equation $16q_6^2 - 3p^x = 1$. We can write

$$3p^x = 16q_6^2 - 1 = (4q_6+1)(4q_6-1).$$

Since $\gcd(4q_6+1, 4q_6-1) = 1$, we obtain four cases: (i) $4q_6+1 = p^x$, $4q_6-1 = 3$, (ii) $4q_6+1 = 3$, $4q_6-1 = p^x$, (iii) $4q_6+1 = 3p^x$, $4q_6-1 = 1$, (iv) $4q_6+1 = 1$, $4q_6-1 = 3p^x$. We easily see that each of these cases is impossible. ∎

Lemma 4.10. *Let p and q_6 be distinct odd prime numbers. Then, for any given positive odd integer d_1, the equation*

$$d_1x^2 + 4q_6^2 = p^y$$

has at most one positive integer solution (x,y).

Proof. We will show

$$(\gamma, d_1, d_2, p) = (1, d_1, 4q_6^2, p) \notin \mathfrak{E}$$

and

$$(d_1, d_2, p) = (d_1, 4q_6^2, p) \notin \mathfrak{F} \cup \mathfrak{G} \cup \mathfrak{H}_1$$

in order to use Theorem 4.4 with $\gamma = 1$.

We easily see that $(1, d_1, 4q_6^2, p) \notin \mathfrak{E}$ and $(d_1, 4q_6^2, p) \notin \mathfrak{G}$. Suppose $(d_1, 4q_6^2, p) \in \mathfrak{F}$. There exists an integer $h > 1$ such that $\mathcal{F}_{h-2\varepsilon} = d_1$, $\mathcal{L}_{h+\varepsilon} = 4q_6^2$, and $\mathcal{F}_h = p$, where $\varepsilon = \pm 1$. For any integer $h \geq 2$, we obtain

$$4\mathcal{F}_h - \mathcal{F}_{h-2\varepsilon} = \mathcal{L}_{h+\varepsilon}$$

(see [1, Lemma 3]). Using this, we obtain

$$4p - d_1 = 4q_6^2.$$

Since $4p - d_1$ is odd, this is impossible. Therefore, $(d_1, 4q_6^2, p) \notin \mathfrak{F}$.

Next suppose $(d_1, 4q_6^2, p) \in \mathfrak{H}_1$. Then $d_1s_0^2 + 4q_6^2 = p^{t_0}$ and $3d_1s_0^2 - 4q_6^2 = \pm 1$ for some positive integers s_0 and t_0. Hence, $16q_6^2 = 3p^{t_0} \pm 1$, contrary to Lemma 4.9. Therefore, $(d_1, 4q_6^2, p) \notin \mathfrak{H}_1$. ∎

Lemma 4.11. *Let p be a prime number such that $p \equiv 1 \bmod 4$ and $2^{p-1} \equiv 1 \bmod p^2$, q_1 a prime factor of $p-2$ such that $q_1^{p-1} \not\equiv 1 \bmod p^2$, n a composite number, and*

$$\alpha := 2q_1 + \sqrt{4q_1^2 - p^n}.$$

Then $\pm\alpha$ is not a p_4th power in $\mathcal{O}_{\mathbb{Q}(\sqrt{4q_1^2-p^n})}$ for any prime p_4 dividing n.

Proof. Suppose $\pm\alpha$ is a p_4th power in $\mathcal{O}_{\mathbb{Q}(\sqrt{4q_1^2-p^n})}$. Since $p \equiv 1 \bmod 4$, we see that $4q_1^2 - p^n \equiv 3 \bmod 4$. Then $\mathcal{O}_{\mathbb{Q}(\sqrt{4q_1^2-p^n})} = \mathbb{Z}[\sqrt{d_0}]$, where d_0 is the square-free part of $4q_1^2 - p^n$. We can write

$$\pm\alpha = (u + v\sqrt{d_0})^{p_4} \tag{4.9}$$

for some integers u and v. First, we assume $p_4 = 2$. Substituting $p_4 = 2$ in (4.9), we have

$$\pm\alpha = (u + v\sqrt{d_0})^2 = (u^2 + v^2 d_0) + 2uv\sqrt{d_0}.$$

On the other hand, we can write

$$4q_1^2 - p^n = c^2 d_0$$

for some positive odd integer c. Using this expression, we have

$$\pm\alpha = \pm 2q_1 \pm c\sqrt{d_0}.$$

Equating the imaginary parts yields

$$\pm c = 2uv.$$

Since c is odd, this is impossible. Thus, $\pm\alpha$ is not a square in $\mathcal{O}_{\mathbb{Q}(\sqrt{4q_1^2-p^n})}$.

Next, we assume $p_4 \geq 3$. It is sufficient to prove that α is not a p_4th power in $\mathcal{O}_{\mathbb{Q}(\sqrt{4q_1^2-p^n})}$. Expanding the right side of $\alpha = (u + v\sqrt{d_0})^{p_4}$, we have

$$\begin{aligned}2q_1 + \sqrt{4q_1^2 - p^n} &= \left\{ \sum_{j=0}^{(p_4-1)/2} \binom{p_4}{2j} u^{p_4-2j} (v^2 d_0)^j \right\} + w\sqrt{d_0} \\ &= u\left\{ \sum_{j=0}^{(p_4-1)/2} \binom{p_4}{2j} u^{p_4-2j-1} (v^2 d_0)^j \right\} + w\sqrt{d_0}\end{aligned}$$

for some integer w. Equating the real parts gives

$$2q_1 = u \sum_{j=0}^{(p_4-1)/2} \binom{p_4}{2j} u^{p_4-2j-1} (v^2 d_0)^j. \tag{4.10}$$

Hence, $u = \pm 1, \pm 2, \pm q_1$, or $\pm 2q_1$. Suppose $u = \pm 1, \pm 2$. Taking the norm of $\alpha = (u + v\sqrt{d_0})^{p_4}$, we have $p^n = (u^2 - v^2 d_0)^{p_4}$. Then $p^{n/p_4} = u^2 - v^2 d_0$, that is,

$$v^2 d_0 = u^2 - p^{n/p_4}.$$

Substituting this in (4.10), we obtain

$$2q_1 = u \sum_{j=0}^{(p_4-1)/2} \binom{p_4}{2j} u^{p_4-2j-1} (u^2 - p^{n/p_4})^j.$$

Since n is a composite number, we have $n/p_4 \geq 2$. Then $p^{n/p_4} \equiv 0 \bmod p^2$. Using this, we see that

$$u\sum_{j=0}^{(p_4-1)/2}\binom{p_4}{2j}u^{p_4-2j-1}(u^2-p^{n/p_4})^j \equiv \sum_{j=0}^{(p_4-1)/2}\binom{p_4}{2j}u^{p_4-2j}u^{2j}$$
$$\equiv u^{p_4}\sum_{j=0}^{(p_4-1)/2}\binom{p_4}{2j} \equiv 2^{p_4-1}u^{p_4} \bmod p^2.$$

Since p is odd, we have

$$q_1 \equiv 2^{p_4-2}u^{p_4} \bmod p^2.$$

Combining this and the assumption $2^{p-1}\equiv 1 \bmod p^2$, we see that

$$q_1^{p-1} \equiv (2^{p_4-2}u^{p_4})^{p-1} \equiv (2^{p_4-2})^{p-1}(u^{p_4})^{p-1}$$
$$\equiv (2^{p-1})^{p_4-2}(u^{p-1})^{p_4} \equiv (u^{p-1})^{p_4} \bmod p^2.$$

If $u=\pm 1$, then $u^{p-1}=1$. If $u=\pm 2$, then $u^{p-1}=2^{p-1}\equiv 1 \bmod p^2$. Then

$$q_1^{p-1} \equiv (u^{p-1})^{p_4} \equiv 1 \bmod p^2,$$

a contradiction. Therefore, $u=\pm q_1$ or $\pm 2q_1$. Suppose $u=\pm q_1$. Substituting this in (4.10), we obtain

$$2q_1 = \pm q_1\sum_{j=0}^{(p_4-1)/2}\binom{p_4}{2j}q_1^{p_4-2j-1}(v^2d_0)^j.$$

Then

$$\pm 2 = \sum_{j=0}^{(p_4-1)/2}\binom{p_4}{2j}q_1^{p_4-2j-1}(v^2d_0)^j \tag{4.11}$$
$$= q_1^{p_4-1} + \sum_{j=1}^{(p_4-1)/2}\binom{p_4}{2j}q_1^{p_4-2j-1}(v^2d_0)^j.$$

Taking the norm of $\alpha = (\pm q_1 + v\sqrt{d_0})^{p_4}$, we get

$$v^2d_0 = q_1^2 - p^{n/p_4}.$$

Since $q_1^2 - p^{n/p_4}$ is even and d_0 is odd, we see that v is even. Then the right side of (4.11) is odd, a contradiction. Therefore, $u=\pm 2q_1$. Taking the norm of $\alpha = (\pm 2q_1 + v\sqrt{d_0})^{p_4}$, we obtain

$$v^2d_0 = 4q_1^2 - p^{n/p_4}.$$

On the other hand,

$$4q_1^2 - p^n = c^2d_0.$$

These imply that both $(x,y)=(c,n)$ and $(x,y)=(|v|,n/p_4)$ are positive integer solutions of $-d_0x^2+4q_1^2=p^y$, contrary to Lemma 4.10. ■

Finally, we show Theorem 4.2(2)(ii) by using Lemma 4.11.

Proof of Theorem 4.2(2)(ii). Since $\gcd(p, 4q_1^2 - p^n) = 1$ and $p \nmid \alpha$, the prime number p splits in $\mathbb{Q}(\sqrt{4q_1^2 - p^n})$. Again

$$(\alpha) = \wp^n,$$

where $\wp$ is the prime ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{4q_1^2-p^n})}$ over p. Let s_1 be the order of the ideal class containing $\wp$. We can write $n = s_1 t_1$ for some integer t_1. Since $\wp^{s_1}$ is principal, there exists $\eta \in \mathcal{O}_{\mathbb{Q}(\sqrt{4q_1^2-p^n})}$ such that $\wp^{s_1} = (\eta)$. Then

$$(\alpha) = (\wp^{s_1})^{t_1} = (\eta)^{t_1} = (\eta^{t_1}).$$

Since $d_0 \equiv -1 \bmod 4$, we have $\mathbb{Q}(\sqrt{4q_1^2 - p^n}) \neq \mathbb{Q}(\sqrt{-3})$. From the assumption $\mathbb{Q}(\sqrt{4q_1^2 - p^n}) \neq \mathbb{Q}(\sqrt{-1})$, we get

$$\mathbb{Q}(\sqrt{4q_1^2 - p^n}) \neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3}).$$

Thus, $\pm\alpha = \eta^{t_1}$. We obtain $t_1 = 1$ by Lemma 4.11. Therefore, $s_1 = n$. ■

REMARK 4.12. We make a remark on Theorem 4.2(2). We will check how often the equality $\mathbb{Q}(\sqrt{4 - p^n}) = \mathbb{Q}(\sqrt{-1})$ (resp. $\mathbb{Q}(\sqrt{4q_1^2 - p^n}) = \mathbb{Q}(\sqrt{-1})$) occurs as n runs over positive integers for a fixed prime number p (resp. for fixed prime numbers p and q_1). The equation

$$x^2 + 4 = p^y$$

has at most one positive integer solution (x, y) except for $p = 5$ (see [15, Lemma 3]). Hence, for a fixed p, there is at most one positive integer n such that $\mathbb{Q}(\sqrt{4 - p^n}) = \mathbb{Q}(\sqrt{-1})$ except for $p = 5$. By Lemma 4.10, the equation

$$x^2 + 4q_1^2 = p^y$$

has at most one positive integer solution (x, y). Thus, for fixed odd prime numbers p and q_1, there is at most one positive integer n such that $\mathbb{Q}(\sqrt{4q_1^2 - p^n}) = \mathbb{Q}(\sqrt{-1})$.

Acknowledgements. The author would like to express her sincere gratitude to Professor Masato Kurihara and Dr. Satoshi Fujii for suggesting this subject and for valuable advice. She would also like to express her gratitude to Professor Dongho Byeon for answering her questions and helpful comments. She has learned a great deal from his papers and it is a pleasure to thank him now. She would like to thank Professor Manabu Ozaki, Professor Hisao Taya, and Dr. Takayuki Morisawa for helpful discussions. Further, she would like to express her thanks to Professor Akio Tamagawa, Professor Yasushi Mizusawa, Professor Tsuyoshi Itoh, and Dr. Filippo Alberto Edoardo Nuccio Mortarino Majno di Capriglio for useful comments. Finally, she is grateful to Professor Kohji Matsumoto for continuous encouragement.

This research was supported by Grant-in-Aid for JSPS Fellows (22-222) from Japan Society for the Promotion of Science.

References

[1] Y. Bugeaud and T. N. Shorey, *On the number of solutions of the generalized Ramanujan–Nagell equation*, J. Reine Angew. Math. 539 (2001), 55–74.

[2] D. Byeon, *A note on basic Iwasawa λ-invariants of imaginary quadratic fields and congruence of modular forms*, Acta Arith. 89 (1999), 295–299.

[3] D. Byeon, *Indivisibility of class numbers and Iwasawa λ-invariants of real quadratic fields*, Compos. Math. 126 (2001), 249–256.

[4] D. Byeon, *A note on the existence of certain infinite families of imaginary quadratic fields*, J. Number Theory 97 (2002), 165–170.

[5] D. Byeon, *Imaginary quadratic fields whose Iwasawa λ-invariant is equal to 1*, Acta Arith. 120 (2005), 145–152.

[6] L. Carlitz, *Arithmetic properties of generalized Bernoulli numbers*, J. Reine Angew. Math. 202 (1959), 174–182.

[7] H. Cohen, *Sums involving the values at negative integers of L-functions of quadratic characters*, Math. Ann. 217 (1975), 271–285.

[8] H. Cohen, *Number Theory. Volume II: Analytic and Modern Tools*, Grad. Texts in Math. 240, Springer, 2007.

[9] J. H. E. Cohn, *Lucas and Fibonacci numbers and some Diophantine equations*, Proc. Glasgow Math. Assoc. 7 (1965), 24–28.

[10] D. S. Dummit, D. Ford, H. Kisilevsky, and J. W. Sands, *Computation of Iwasawa lambda invariants for imaginary quadratic fields*, J. Number Theory 37 (1991), 100–121.

[11] J. S. Ellenberg, S. Jain, and A. Venkatesh, *Modeling λ-invariants by p-adic random matrices*, Comm. Pure Appl. Math. 64 (2011), 1243–1262.

[12] T. Fukuda and H. Taya, *Computation of Iwasawa invariants*, Nihon Oyo Surigakkai Ronbunshi 12 (2002), 293–306.

[13] R. Gold, *The nontriviality of certain $\mathbb{Z}_l$-extensions*, J. Number Theory 6 (1974), 369–373.

[14] K. Ishii, *On the divisibility of the class number of imaginary quadratic fields*, Proc. Japan Acad. Ser. A Math. Sci. 87 (2011), 142–143.

[15] A. Ito, *Remarks on the divisibility of the class numbers of imaginary quadratic fields* $\mathbb{Q}(\sqrt{2^{2k}-q^n})$, Glasgow Math. J. 53 (2011), 379–389.

[16] A. Ito, *Notes on the divisibility of the class numbers of the imaginary quadratic fields* $\mathbb{Q}(\sqrt{3^{2e}-4k^n})$, arXiv:1212.1733 (2012).

[17] K. James and K. Ono, *Selmer groups of quadratic twists of elliptic curves*, Math. Ann. 314 (1999), 1–17.

[18] Y. Kida, *On cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields*, Tôhoku Math. J. 31 (1979), 91–96.

[19] I. Kimura, *A note on the existence of certain infinite families of imaginary quadratic fields*, Acta Arith. 110 (2003), 37–43; Corrigendum, ibid. 114 (2004), 397.

[20] Y. Kishi, *Note on the divisibility of the class number of certain imaginary quadratic fields*, Glasgow Math. J. 51 (2009), 187–191; Corrigendum, ibid. 52 (2010), 207–208.

[21] W. Kohnen and K. Ono, *Indivisibility of class numbers of imaginary quadratic fields and orders of Tate–Shafarevich groups of elliptic curves with complex multiplication*, Invent. Math. 135 (1999), 387–398.

[22] J. S. Kraft and L. C. Washington, *Heuristics for class numbers and lambda invariants*, Math. Comp. 76 (2007), 1005–1023.

[23] M.-G. Leu and G.-W. Li, *The Diophantine equation* $2x^2+1=3^n$, Proc. Amer. Math. Soc. 131 (2003), 3643–3645.

[24] Y. Mizusawa, http://mizusawa.web.nitech.ac.jp/Iwapoly/index.html.

[25] K. Ono, *Indivisibility of class numbers of real quadratic fields*, Compos. Math. 119 (1999), 1–11.

[26] J. W. Sands, *On the nontriviality of the basic Iwasawa λ-invariant for an infinitude of imaginary quadratic fields*, Acta Arith. 65 (1993), 243–248.

[27] J. Sturm, *On the congruence of modular forms*, in: Number Theory (New York, 1984–1985), Lecture Notes in Math. 1240, Springer, Berlin, 1987, 275–280.

[28] L. C. Washington, *Zeros of p-adic L-functions*, in: Séminaire Delange–Pisot–Poitou (Séminaire de Théorie des Nombres, Paris, 1980/1981), Progr. Math. 22, Birkhäuser, Boston, 1982, 337–357.

[29] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.

Akiko Ito
Kanagawa University
3-27-1, Rokkakubashi, Kanagawa-ku
Yokohama-shi, Kanagawa, 221-8686, Japan
E-mail: aito@kanagawa-u.ac.jp

Received on 17.8.2012
and in revised form on 28.2.2015 (7162)