SUMS OF QUADRATIC FUNCTIONS WITH TWO DISCRIMINANTS AND FARKAS' IDENTITIES WITH QUARTIC CHARACTERS

A DISSERTATION SUBMITTED TO THE OFFICE OF GRADUATE EDUCATION OF THE
UNIVERSITY OF HAWAI'I AT MĀNOA IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

MATHEMATICS

AUGUST 2017

By

Ka Lun Wong

Dissertation Committee:

Pavel Guerzhoy, Chairperson
Michelle Manes
Robert Harron
Paul Jenkins
Dusko Pavlovic

Keywords: dissertations, mathematics, number theory, modular forms

To my dear parents,

Wah Wong and Yim Ming Loong,

and my beloved wife,

Carol

ACKNOWLEDGMENTS

I want to thank my advisor, Professor Pavel Guerzhoy, for his tremendous help throughout my PhD study. I really appreciate his ideas and suggestions for my dissertation projects. He has been a tremendous guide through the challenges and problems that come with obtaining a PhD, and he has always been available to me whenever I needed help. He is very patient and willing to go over any subjects or problems I struggle with. He also has been a priceless source of advice, especially regarding giving talks and writing papers.

I also want to thank Professor Michelle Manes for her constant support in my study. She has been a truly wonderful resource in every way.

Thanks as well to my wife Carol. She has sacrificed so much to help me fulfill my dream to earn a PhD. She is always by my side, ready to cheer me up, support me, and encourage me, whatever challenges might come our way. I couldn't have done this without her.

ABSTRACT

Zagier in [21] discusses a construction of a function $F_{k,D}(x)$ defined for an even integer $k \geq 2$, and a positive discriminant D. This construction is intimately related to half-integral weight modular forms. In particular, the average value of this function is a constant multiple of the D-th Fourier coefficient of weight $k + 1/2$ Eisenstein series constructed by H. Cohen in [2].

In this dissertation, we consider a construction which works both for even and odd positive integers k. Our function $F_{k,D,d}(x)$ depends on two discriminants d and D with signs $\text{sign}(d) = \text{sign}(D) = (-1)^k$, degenerates to Zagier's function when $d = 1$, namely,

$$F_{k,D,1}(x) = F_{k,D}(x),$$

and has very similar properties. In particular, we prove that the average value of $F_{k,D,d}(x)$ is again a Fourier coefficient of H. Cohen's Eisenstein series of weight $k + 1/2$, while now the integer $k \geq 2$ is allowed to be both even and odd.

In [6] Farkas introduces a new arithmetic function and proves an identity involving this function. Guerzhoy and Raji [8] generalize this function for primes that are congruent to 3 modulo 4 by introducing a quadratic Dirichlet character and find another identity of the same type. We look at the case when $p \equiv 5 \pmod 8$ by introducing quartic Dirichlet characters and prove an analogue of their generalization.

TABLE OF CONTENTS

Acknowledgments . . . **iv**

Abstract . . . **v**

1 Background materials . . . **1**

1.1 Elementary number theory . . . 1

1.1.1 The Kronecker symbol . . . 1

1.1.2 L-functions associated to quadratic fields . . . 3

1.1.3 Polynomial congruences . . . 5

1.2 Modular Forms . . . 6

2 Sums of Quadratic Functions with two Discriminants . . . **13**

2.1 Introduction . . . 13

2.2 Basic Properties of $F_{k,D,d}(x)$ . . . 16

2.3 Proof of Theorem 2.1 . . . 23

2.4 Proofs of Propositions 2.7 and 2.8 . . . 27

2.4.1 Case 1(i)(a) . . . 29

2.4.2 Case 1(i)(b) . . . 31

2.4.3 Case 1(ii) and 1(iii) . . . 32

2.4.4 Case 1(iv)(a) . . . 34

2.4.5 Case 1(iv)(b) . . . 40

2.4.6 Case 2(i)(a) . . . 54

2.4.7 Case 2(i)(b) . . . 60

2.4.8 Case 2(ii)(a) . . . 64

2.4.9 Case 2(ii)(b) 66

2.4.10 Case 2(iii)(a) 69

2.4.11 Case 2(iii)(b) 75

2.4.12 Case 2(iv)(a) 81

2.4.13 Case 2(iv)(b) 85

2.5 Proof of Theorem 2.2 98

3 Farkas' Identities with Quartic Characters 101

3.1 Introduction 101

3.2 Proofs of the main facts 104

3.3 Squaring the generating function of δ_χ 110

3.4 Even characters 117

A Dimension 123

Bibliography 125

CHAPTER 1
BACKGROUND MATERIALS

We begin with a preliminary chapter that gives some basic definitions and theorems from number theory. We will introduce some elementary number theory in the first section. Then we will introduce the theory of modular forms in the second section.

1.1 Elementary number theory

1.1.1 The Kronecker symbol

In this section, we will use [1], [3] and [5] as our references. For any positive integer N, let G_N denote the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$. A *Dirichlet character modulo* N is a homomorphism of multiplicative groups,

$$\chi : G_N \to \mathbb{C}^*.$$

The set of Dirichlet characters forms a group under multiplication, $(\chi\psi)(n) = \chi(n)\psi(n)$. We denote the Dirichlet character group by $\hat{G}_N$, called the dual group.

Proposition 1.1. *Let $\hat{G}_N$ be the dual group of G_N. Then $\hat{G}_N$ is isomorphic to G_N. In particular, the number of Dirichlet character modulo N is $\phi(N)$ where ϕ is the Euler totient.*

Every Dirichlet character χ modulo N extends to a function $\chi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ where $\chi(n) = 0$ for noninvertible elements n of the ring $\mathbb{Z}/N\mathbb{Z}$, and then extends further to a function $\chi : \mathbb{Z} \to \mathbb{C}$ where $\chi(n) = \chi(n \mod N)$ for all $n \in \mathbb{Z}$.

Definition 1.2. *Let χ be a Dirichlet character modulo N.*

*(1) If $d|N$, we say that χ **can be defined modulo** d if there exists a Dirichlet character χ_d modulo d such that $\chi(n) = \chi_d(n)$ as soon as $gcd(n, N) = 1$.*

*(2) The **conductor** of a Dirichlet character is the smallest (for divisibility) positive integer $f|N$ such that χ can be defined modulo f.*

*(3) We say that χ is **primitive** if the conductor of χ is equal to N.*

Now, we will define a function called the Kronecker symbol which is a real Dirichlet character in certain cases. Let n be a non-zero integer with prime factorization $n = up_1^{e_1} \cdots p_r^{e_r}$, where $u = \pm 1$, and the p_i are primes. Let a be an integer. The *Kronecker symbol* $\left(\frac{a}{n}\right)$ is defined by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{u}\right) \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{e_i},$$

where $\left(\frac{a}{p_i}\right)$ is the Legendre symbol if p_i is odd, i.e.,

$$\left(\frac{a}{p_i}\right) = \begin{cases} 1 & \text{if } p_i \nmid a \text{ and } a \text{ is a square mod } p_i, \\ -1 & \text{if } p_i \nmid a \text{ and } a \text{ is not a square mod } p_i, \\ 0 & \text{if } p_i | a. \end{cases}$$

For $p_i = 2$, define

$$\left(\frac{a}{2}\right) = \begin{cases} 1 & \text{if } a \equiv \pm 1 \pmod 8, \\ -1 & \text{if } a \equiv \pm 3 \pmod 8, \\ 0 & \text{if } 2|a. \end{cases}$$

Also, we define $\left(\frac{a}{1}\right) = 1$ and

$$\left(\frac{a}{-1}\right) = \begin{cases} 1 & \text{if } a \geq 0, \\ -1 & \text{if } a < 0. \end{cases}$$

Finally, we define

$$\left(\frac{a}{0}\right) = \begin{cases} 1 & \text{if } a = \pm 1, \\ 0 & \text{if otherwise.} \end{cases}$$

To characterize real primitive Dirichlet characters, we define the following terms. An integer D is called a *discriminant* if $D \equiv 0$ or $1 \pmod 4$. An integer d is called a *fundamental discriminant* if

- $d \equiv 1 \pmod 4$ and is square-free, or
- $d = 4m$, where $m \equiv 2$ or $3 \pmod 4$ and m is square-free.

We have the following theorem (see [3, Theorem 2.2.15]).

Theorem 1.3. *If d is a fundamental discriminant, the Kronecker symbol $\left(\frac{d}{n}\right)$ defines a real primitive Dirichlet character modulo $N = |d|$. Conversely, if χ is a real primitive character modulo N then $d = \chi(-1)N$ is a fundamental discriminant and $\chi(n) = \left(\frac{d}{n}\right)$.*

Specifically, if p is a prime congruent to 1 modulo 4, then $\chi(n) = \left(\frac{p}{n}\right)$ is a real primitive (quadratic) Dirichlet character.

The following proposition (see [3, Proposition 2.2.6]) is known as quadratic reciprocity.

Proposition 1.4. *For two nonzero integers m and n write $m = 2^{v_2(m)}m_1$ and $n = 2^{v_2(n)}n_1$ with m_1 and n_1 odd. Then*

$$\left(\frac{n}{m}\right) = (-1)^{\frac{(m_1-1)(n_1-1)+(\mathrm{sign}(m)-1)(\mathrm{sign}(n)-1)}{4}} \left(\frac{m}{n}\right).$$

Here we give a proposition related to a sum of Kronecker symbols.

Proposition 1.5. *Let p be an odd prime. Then*

$$\sum_{y=0}^{p-1} \left(\frac{y^2+a}{p}\right) = \begin{cases} -1 & \text{if} \quad p \nmid a, \\ p-1 & \text{if} \quad p|a. \end{cases} \tag{1.1}$$

Proof. The equation $x^2 - y^2 \equiv a \pmod p$ or $x^2 \equiv y^2 + a \pmod p$ has $\sum_{y=0}^{p-1}\left(1+\left(\frac{y^2+a}{p}\right)\right)$ solutions because as y runs through 1 to p, if $y^2+a \neq 0$ is a square mod p, then there are two solutions x and $-x$. Otherwise, it has no solution. And if $y^2+a=0$, there is only one solution for x. On the other hand, let $u = x+y$ and $v = x-y$. The equation becomes $uv \equiv a \pmod p$. If $p \nmid a$, the solutions are $1 \cdot a$, $2 \cdot \frac{a}{2}, ..., (p-1) \cdot \frac{a}{p-1}$. Each solution (u, v) gives a solution to (x, y). Thus, there are $p-1$ solutions. If $p|a$, then $uv \equiv 0 \pmod p$. The solutions are $u = 0$ and $v = 1, 2, ..., p-1$ or $v = 0$ and $u = 1, 2, ..., p-1$ or $u = v = 0$. Thus there are $2p-1$ solutions. Therefore,

$$\sum_{y=0}^{p-1}\left(1+\left(\frac{y^2+a}{p}\right)\right) = p + \sum_{y=0}^{p-1}\left(\frac{y^2+a}{p}\right) = \begin{cases} p-1 & \text{if} \quad p \nmid a, \\ 2p-1 & \text{if} \quad p|a, \end{cases}$$

and thus,

$$\sum_{y=0}^{p-1}\left(\frac{y^2+a}{p}\right) = \begin{cases} -1 & \text{if} \quad p \nmid a, \\ p-1 & \text{if} \quad p|a \end{cases}$$

as required. □

1.1.2 L-functions associated to quadratic fields

Now, we will quote some formulas and theorems related to the gamma function from [1] which will be used in later chapters. For $z \in \mathbb{C}$ with $\Re(z) > 0$, let $\Gamma(z)$ be the gamma function defined by

$$\Gamma(z) = \int_0^\infty x^{z-1} e^{-x} dx.$$

Extend this function by analytic continuation to all complex numbers except the non-positive integers. From [1, p.260], we have, for all $s \in \mathbb{C}$,

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s), \tag{1.2}$$

where $\zeta(s)$ is the Riemann zeta function,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Replacing s by $2s$ in (1.2), we get

$$\frac{1}{\zeta(2s)} = \frac{\Gamma(s)}{\pi^{2s-\frac{1}{2}}\Gamma\left(\frac{1-2s}{2}\right)\zeta(1-2s)}. \tag{1.3}$$

We also have

$$\Gamma\left(\frac{s}{2}\right)\Gamma\left(1-\frac{s}{2}\right) = \frac{\pi}{\sin\frac{\pi s}{2}}. \tag{1.4}$$

If we replace s by $1+2k$ where k is an integer, then we can get

$$\Gamma\left(\frac{1}{2}+k\right)\Gamma\left(\frac{1}{2}-k\right) = (-1)^k\pi. \tag{1.5}$$

Here is another formula:

$$2^s\pi^{1/2}\Gamma(1-s) = \Gamma\left(\frac{1-s}{2}\right)\Gamma\left(1-\frac{s}{2}\right). \tag{1.6}$$

Substitute $s = 1-k$ and then square the equation, we get

$$\frac{\Gamma(k)^2}{\Gamma\left(\frac{k+1}{2}\right)^2} = \frac{\Gamma\left(\frac{k}{2}\right)^2}{2^{2-2k}\pi}. \tag{1.7}$$

For each fundamental discriminant d, we define two Dirichlet series. Let $\chi_d(n) = \left(\frac{d}{n}\right)$. For $s \in \mathbb{C}$ with $\Re(s) > 1$, we define the *Dirichlet L-series* with χ_d and the *Dedekind zeta-function* by

$$L_d(s) = L(s,\chi_d) = \sum_{n=1}^{\infty} \frac{\chi_d(n)}{n^s}, \text{ and } \zeta_d(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s},$$

where the second sum is over all non-zero ideals $\mathfrak{a}$ in the ring of integers of $K = \mathbb{Q}(\sqrt{d})$ and $N(\mathfrak{a})$ is the norm of the ideal. For other $s \in \mathbb{C}$, they are defined by analytic continuation. For any discriminant D, see [20] and [21] for general definitions and properties of $L_D(s)$ and $\zeta_D(s)$.

Here we give two functional equations and a relation for any discriminant D (see [21]):

$$L_D(1-s) = \frac{|D|^{s-1/2}\Gamma\left(\frac{s}{2}\right)}{\pi^{s-1/2}\Gamma\left(\frac{1-s}{2}\right)} L_D(s), \tag{1.8}$$

$$\zeta_D(1-s) = \frac{|D|^{s-1/2}\Gamma\left(\frac{s}{2}\right)^2}{\pi^{2s-1}\Gamma\left(\frac{1-s}{2}\right)^2} \zeta_D(s), \tag{1.9}$$

$$\zeta_D(s) = \zeta(s) L_D(s). \tag{1.10}$$

1.1.3 Polynomial congruences

Now, we will quote two theorems related to polynomial congruences. See [1, Theorem 5.28] for the following one which is a consequence of the Chinese remainder theorem.

Theorem 1.6. *Let f be a polynomial with integer coefficients, let $m_1, m_2, ..., m_r$ be positive integers relatively prime in pairs, and let $m = m_1 m_2 \cdots m_r$. Then the congruence*

$$f(x) \equiv 0 \pmod{m} \tag{1.11}$$

has a solution if, and only if, each of the congruences

$$f(x) \equiv 0 \pmod{m_i} \quad (i = 1, 2, ..., r) \tag{1.12}$$

has a solution. Moreover, if $v(m)$ and $v(m_i)$ denote the number of solutions of (1.11) and (1.12), respectively, then

$$v(m) = v(m_1)v(m_2)\cdots v(m_r). \tag{1.13}$$

For the following, see [1, Theorem 5.30].

Theorem 1.7. *Let p be prime. Assume $\alpha \geq 2$ and let r be a solution of the congruence*

$$f(x) \equiv 0 \pmod{p^{\alpha-1}}$$

lying in the interval $0 \leq r < p^{\alpha-1}$.
(a) Assume $f'(r) \not\equiv 0 \pmod{p}$. Then r can be lifted in a unique way from $p^{\alpha-1}$ to p^α. That is, there is a unique a in the interval $0 \leq a < p^\alpha$ congruent to r mod $p^{\alpha-1}$ such that a satisfies the congruence

$$f(x) \equiv 0 \pmod{p^\alpha}. \tag{1.14}$$

(b) Assume $f'(r) \equiv 0 \pmod{p}$. Then we have two possibilities:
(b_1) If $f(r) \equiv 0 \pmod{p^\alpha}$, r can be lifted from $p^{\alpha-1}$ to p^α in p distinct ways.
(b_2) If $f(r) \not\equiv 0 \pmod{p^\alpha}$, r cannot be lifted from $p^{\alpha-1}$ to p^α.

Theorem 1.7 is also known as Hensel's lemma.

1.2 Modular Forms

In this section, we will give a brief overview of the theory of modular forms. We will use [5], [10] and [22] as our references. Let $\mathfrak{H}$ be the upper half complex plane, i.e.,

$$\mathfrak{H} = \{z \in \mathbb{C} | \Im(z) > 0\}.$$

Let $\mathrm{SL}_2(\mathbb{Z})$ be the group of 2×2 matrices with integer coefficients with determinant 1. We also call $\mathrm{SL}_2(\mathbb{Z})$ the full modular group. It acts on $\mathfrak{H}$ by Möbius transformations, i.e., for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$,

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \mathfrak{H} \to \mathfrak{H}, \qquad z \mapsto \gamma z = \frac{az+b}{cz+d}.$$

To see that the action is well-defined, we compute

$$\Im(\gamma z) = \frac{\Im(z)}{|cz+d|^2}.$$

Since the denominator is positive, we know that $\gamma z \in \mathfrak{H}$.

Definition 1.8. *Let k be an integer. A holomorphic function $f : \mathfrak{H} \to \mathbb{C}$ is a **modular form of weight** k for $\mathrm{SL}_2(\mathbb{Z})$ if*

(1) f satisfies

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \tag{1.15}$$

for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, and

(2) f is holomorphic at ∞.

We will explain what it means for f to be holomorphic at ∞ in the following. Since f satisfies (1.15) for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, it satisfies (1.15) for $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ specifically, i.e., $f(x+1) = f(x)$. Thus, f is periodic with period 1 and has a Fourier expansion in a neighborhood of the origin:

$$f(q) = \sum_{n \in \mathbb{Z}} a_n q^n, \text{ with } q := e^{2\pi i z}.$$

If $a_n = 0$ for $n < 0$, then we say f is holomorphic at ∞. If $a_n = 0$ for $n < -N$ for some positive integer N, we say f is meromorphic at ∞.

Let N be a positive integer. The *principal congruence subgroup of level N* is

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Definition 1.9. *A subgroup* Γ *of* $\mathrm{SL}_2(\mathbb{Z})$ *is a* ***congruence subgroup*** *if* $\Gamma(N) \subset \Gamma$ *for some* $N \in \mathbb{Z}^+$*, in which case* Γ *is a congruence subgroup of level* N*.*

The following are two important congruence subgroups:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

We have

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z}) = \Gamma(1).$$

Now, for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ and any integer k, we define the *weight-k operator* $[\gamma]_k$ on functions $f : \mathfrak{H} \to \mathbb{C}$ by

$$(f[\gamma]_k)(z) = (cz+d)^{-k} f(\gamma z), \quad z \in \mathfrak{H}.$$

We also say f is weight-k invariant under a congruence subgroup Γ if

$$f[\gamma]_k = f \text{ for all } \gamma \in \Gamma.$$

Now we can define a modular form of weight k with respect to a congruence subgroup. To avoid some technical details, we restrict our congruence subgroups to those that contain $\Gamma_1(N)$ throughout this chapter.

Definition 1.10. *Let* Γ *be a congruent subgroup of* $\Gamma(1)$ *and let* k *be an integer. A holomorphic function* $f : \mathfrak{H} \to \mathbb{C}$ *is a* ***modular form of weight*** k ***with respect to*** Γ *if*

(1) f *is weight-k invariant under* Γ*,*

(2) $f[\gamma]_k$ *is holomorphic at* ∞ *for all* $\gamma \in \Gamma(1)$*.*

Note: We say $f[\gamma]_k$ *is* ***holomorphic at*** ∞ *if the Fourier expansion of* $f[\gamma]_k$ *(over* $q^{1/N}$*) has coefficients* $a_n = 0$ *for* $n < 0$*. Condition (2) above is sometimes phrased* f *is holomorphic at all cusps. If in addition,* $a_0 = 0$ *in the Fourier expansion of* $f[\gamma]_k$ *for all* $\gamma \in \Gamma(1)$*, then* f *is a* ***cusp form*** *of weight* k *with respect to* Γ*.*

We denote the set of modular forms and cusp forms of weight k with respect to Γ by $M_k(\Gamma)$ and $S_k(\Gamma)$ respectively. The set $M_k(\Gamma)$ of modular forms of weight k with respect to Γ forms a vector space over $\mathbb{C}$ and the set $S_k(\Gamma)$ forms a vector subspace of $M_k(\Gamma)$. Even more, $M_k(\Gamma)$ forms a finite dimensional vector space. The dimension formulas can be found, for example, in [17, Chapter 6].

Proposition 1.11. *Let k and l be integers and Γ be some congruence subgroup of $\Gamma(1)$. If $f \in M_k(\Gamma)$ and $g \in M_l(\Gamma)$, then $fg \in M_{k+l}(\Gamma)$.*

Now, for each Dirichlet character χ modulo N, define the χ-*eigenspace* of $M_k(\Gamma_1(N))$,

$$M_k(N,\chi) = \{f \in M_k(\Gamma_1(N)) : f[\gamma]_k = \chi(d_\gamma)f \text{ for all } \gamma \in \Gamma_0(N)\}.$$

Here d_γ denotes the lower right entry of γ. In particular, the eigenspace $M_k(N, \mathbf{1}_N)$ is $M_k(\Gamma_0(N))$ where $\mathbf{1}_N$ denotes the principal character modulo N. Note that $M_k(N,\chi)$ is just $\{0\}$ unless $\chi(-1) = (-1)^k$. It is also true that $M_k(\Gamma_1(N))$ decomposes as the direct sum of the eigenspaces,

$$M_k(\Gamma_1(N)) = \bigoplus_{\chi} M_k(N,\chi).$$

Proposition 1.12. *Let k and l be integers. Let N be a positive integer, χ and ψ be Dirichlet characters modulo N. If $f \in M_k(N,\chi)$ and $g \in M_l(N,\psi)$, then $fg \in M_{k+l}(N,\chi\psi)$.*

From the definition of modular forms of weight k with respect to a congruence subgroup, we can see that $M_k(\Gamma_1(N)) \supset M_k(\Gamma_0(N))$. We will now introduce an operator, called Hecke operator, on the larger space $M_k(\Gamma_1(N))$. Denote $\mathrm{GL}_2^+(\mathbb{Q})$ the group of 2-by-2 matrices with rational entries and positive determinant. We define the following.

Definition 1.13. *For congruence subgroups Γ_1 and Γ_2 of $\Gamma(1)$ and $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, the **weight**-$k$ $\Gamma_1\alpha\Gamma_2$ **operator** takes functions $f \in M_k(\Gamma_1)$ to*

$$f[\Gamma_1\alpha\Gamma_2]_k = \sum_j f[\beta_j]_k$$

where $\{\beta_j\}$ are orbit representatives, i.e., $\Gamma_1\alpha\Gamma_2 = \bigcup_j \Gamma_1\beta_j$ is a disjoint union.

The double coset operator is well defined, i.e., it is independent of how the β_j are chosen. It takes modular forms with respect to Γ_1 to modular forms with respect to Γ_2,

$$[\Gamma_1\alpha\Gamma_2]_k : M_k(\Gamma_1) \to M_k(\Gamma_2).$$

It also takes cusp forms to cusp forms,

$$[\Gamma_1\alpha\Gamma_2]_k : S_k(\Gamma_1) \to S_k(\Gamma_2).$$

Now, the pth Hecke operator is a weight-k double coset operator $[\Gamma_1\alpha\Gamma_2]_k$ where $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$, with

$$\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}, \quad p \text{ prime}.$$

This operator is denoted T_p. Thus,

$$T_p : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N)), \;\; p \text{ prime}$$

is given by

$$T_p f = f[\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N)]_k.$$

To describe the effect of T_p on Fourier coefficients, see the following [5, Proposition 5.2.2].

Proposition 1.14. *Let $f \in M_k(\Gamma_1(N))$ with a Fourier expansion*

$$f(z) = \sum_{n=1}^{\infty} a_n(f) q^n, \;\; q = e^{2\pi i z}.$$

Let χ be a Dirichlet character modulo N. If $f \in M_k(N, \chi)$, then also $T_p f \in M_k(N, \chi)$, and its Fourier expansion is

$$T_p f(z) = \sum_{n=1}^{\infty} a_{np}(f) q^n + \chi(p) p^{k-1} \sum_{n=1}^{\infty} a_n(f) q^{np}.$$

For an arbitrary positive integer n, T_n can be defined inductively if n is a prime power and multiplicatively for all n. To keep it simple, we will not include the definition here. A non-zero modular form $f \in M_k(\Gamma_1(N))$ is called a *Hecke eigenform* if it is a simultaneous eigenform for the Hecke operators T_n for all $n \in \mathbb{Z}^+$, i.e., for each $n \in \mathbb{Z}^+$,

$$T_n f = c_n f,$$

for some $c_n \in \mathbb{C}$.

Now, we will introduce an inner product on the space of cusp forms $S_k(\Gamma_1(N))$. Define the hyperbolic measure on the upper half plane,

$$d\mu(\tau) = \frac{dxdy}{y^2}, \;\; \tau = x + iy \in \mathfrak{H}.$$

For a congruence subgroup Γ of $\Gamma(1)$, we define the *modular curve* $Y(\Gamma)$ as the quotient space of orbits under Γ,

$$Y(\Gamma) = \Gamma \setminus \mathfrak{H} = \{\Gamma\tau : \tau \in \mathfrak{H}\}.$$

To compactify the modular curve $Y(\Gamma) = \Gamma \setminus \mathfrak{H}$, define $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\}$ and take the extended quotient

$$X(\Gamma) = \Gamma \setminus \mathfrak{H}^* = Y(\Gamma) \cup \Gamma \setminus (\mathbb{Q} \cup \{\infty\}).$$

Define the volume of $X(\Gamma)$ to be

$$V_\Gamma = \int_{X(\Gamma)} d\mu(\tau)$$

Now, we are ready to define the inner product on cusp forms.

Definition 1.15. *Let $\Gamma \subset \Gamma(1)$ be a congruence subgroup. The* ***Petersson inner product****,*

$$\langle \cdot, \cdot \rangle_\Gamma : S_k(\Gamma) \times S_k(\Gamma) \to \mathbb{C},$$

is given by

$$\langle f, g \rangle_\Gamma = \frac{1}{V_\Gamma} \int_{X(\Gamma)} f(\tau)\overline{g(\tau)}(\Im(\tau))^k d\mu(\tau).$$

The following theorem (see [5, Theorem 5.5.4]) tells us the existence of an orthogonal basis of Hecke eigenforms.

Theorem 1.16. *The space $S_k(\Gamma_1(N))$ has an orthogonal basis of simultaneous eigenforms for the Hecke operators $\{T_n : (n, N) = 1\}$.*

Before we move to half integral weight modular forms, we want to introduce the L-functions of modular forms of integral weight. For a modular form $f = \sum_{n=0}^{\infty} a_n q^n \in M_k(\Gamma_1(N))$ and a Dirichlet character χ, the associated L-functions are defined as the analytic continuations of

$$L(s, f) = \sum_{n=0}^{\infty} a_n n^{-s}, \qquad L(s, f, \chi) = \sum_{n=0}^{\infty} \chi(n) a_n n^{-s}.$$

Convergence of $L(s, f)$ in a half plane of s-values follows from estimating the Fourier coefficients of f. We give the following proposition (see [5, Proposition 5.9.1]).

Proposition 1.17. *If $f \in M_k(\Gamma_1(N))$ is a cusp form, then $L(s, f)$ converges absolutely for all s with $\Re(s) > k/2 + 1$. If f is not a cusp form, then $L(s, f)$ converges absolutely for all s with $\Re(s) > k$.*

We will now introduce half integral weight modular forms (see [13]). To define these forms, we let $\left(\frac{c}{d}\right)$ be the Kronecker symbol and define the symbol ϵ_d. Define ϵ_d, for odd d, by

$$\epsilon_d := \begin{cases} 1 & \text{if } d \equiv 1 \pmod 4, \\ i & \text{if } d \equiv 3 \pmod 4. \end{cases}$$

Here, we let $\sqrt{z}$ be the branch of the square root having argument in $(-\pi/2, \pi/2]$. Hence, $\sqrt{z}$ is a holomorphic function on the complex plane with negative real axis removed.

Definition 1.18. *Suppose that λ is a nonnegative integer and that N is a positive integer. Furthermore, suppose that χ is a Dirichlet character modulo $4N$. A meromorphic function $g(z)$ on $\mathfrak{H}$ is called a* ***meromorphic half-integral weight modular form with Nebentypus*** *χ and weight $\lambda + \frac{1}{2}$ if it is meromorphic at the cusps of $\Gamma_0(4N)$, and if*

$$g\left(\frac{az+b}{cz+d}\right) = \chi(d)\left[\left(\frac{c}{d}\right)\right]^{2\lambda+1} \epsilon_d^{-1-2\lambda}(cz+d)^{\lambda+\frac{1}{2}} g(z)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4N)$. If $g(z)$ is holomorphic on $\mathfrak{H}$ and at the cusps of $\Gamma_0(4N)$, then $g(z)$ is referred to as a (holomorphic) half-integral weight modular form.

We denote the $\mathbb{C}$-vector space of weight $\lambda + \frac{1}{2}$ modular forms on $\Gamma_0(4N)$ with Nebentypus χ by

$$M_{\lambda+\frac{1}{2}}(\Gamma_0(4N), \chi).$$

If χ is the trivial character modulo $4N$, then we use the notation

$$M_{\lambda+\frac{1}{2}}(\Gamma_0(4N)).$$

The theta-function $\theta_0(\tau)$ given by the Fourier series

$$\theta_0(\tau) := \sum_{n=-\infty}^{\infty} q^{n^2} = 1 + 2q + 2q^4 + 2q^9 + \cdots, \quad q = e^{2\pi i \tau},$$

provides the first example of a half integral weight modular form. See [13, Proposition 1.31].

Proposition 1.19. *We have that*

$$\theta_0(\tau) \in M_{\frac{1}{2}}(\Gamma_0(4)).$$

The idea of a half integral weight modular form is that when you square it, it becomes an integral weight modular form. In this case, $\theta_0(z)^2$ is a modular form of weight one.

In [2], Cohen defined some numbers, denoted by $H(k, N)$, with k and N non-negative integers. We call them Cohen's numbers here. They are equal to values of Dirichlet L-functions at negative integers, up to some constant multiples. More importantly, they are coefficients of certain modular forms of half integral weight.

Let k and N be non-negative integers with $k \geq 1$. For $N \geq 1$, we define

$$h(k, N) = \begin{cases} (-1)^{[k/2]}(k-1)! N^{k-1/2} 2^{1-k} \pi^{-k} L(k, \chi_{(-1)^k N}) & \text{if } (-1)^k N \equiv 0 \text{ or } 1 \pmod 4, \\ 0 & \text{if } (-1)^k N \equiv 2 \text{ or } 3 \pmod 4, \end{cases} \tag{1.16}$$

where we write χ_D for the character $\chi_D(d) = \left(\frac{D}{d}\right)$.

Define

$$H(k,N) = \begin{cases} \sum_{d^2|N} h(k,N/d^2) & \text{if } (-1)^k N \equiv 0 \text{ or } 1 \pmod 4, \quad N>0, \\ \zeta(1-2k) & \text{if } N=0, \\ 0 & \text{otherwise.} \end{cases} \tag{1.17}$$

A few facts (see [2]) about Cohen's numbers are:

a) $H(k,N)$ are rational numbers.

b) If $D=(-1)^r N$ is a fundamental discriminant,

$$H(k,N) = L(1-k,\chi_D).$$

c) More generally if we set $(-1)^k N = Df^2$ with a fundamental discriminant D, we have

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

where μ is the Möbius function and σ_x is the sum of positive divisors to the x-th power function.

Now, set

$$\mathcal{H}_k(\tau) = \sum_{N\geq 0} H(k,N)q^N \ \text{ with } q=e^{2\pi i\tau}.$$

Then we have the following theorem (see [2, Theorem 3.1]),

Theorem 1.20. *For $k\geq 2$, $\mathcal{H}_k(\tau)\in M_{k+1/2}(\Gamma_0(4))$.*

CHAPTER 2
SUMS OF QUADRATIC FUNCTIONS WITH TWO DISCRIMINANTS

2.1 Introduction

Let $\mathfrak{Q}_D$ be the set of all quadratic functions $Q = ax^2 + bx + c = [a, b, c]$ with integer coefficients and of non-square discriminant $D = b^2 - 4ac > 0$. For an even positive integer $k \geq 2$, Zagier [21] defines the function $F_{k,D} : \mathbb{R} \to \mathbb{R}$ by

$$F_{k,D}(x) := \sum_{\substack{Q \in \mathfrak{Q}_D \\ a<0<Q(x)}} Q(x)^{k-1}$$

and investigates its striking properties, including the following:

- For fixed D and k, with k small, the function $F_{k,D}(x)$ is constant.
- For fixed D and k, $F_{k,D}(x)$, being a periodic function, has an average value related to values of the Riemann zeta function and Dirichlet L-functions.
- For a fixed k and a fixed input x, $F_{k,D}(x)$ are coefficients of a half integral weight modular form as D varies.

The construction raises an obvious question, what happens if k is odd: the function $F_{k,D}(x)$ fails to have all these properties then. In [21, Section 9], Zagier explains how one can gain the extra freedom and allow k to be odd: he suggests to consider a symmetrization

$$F_{k,\mathcal{A}}(x) := \sum_{\substack{Q \in \mathcal{A} \\ a<0<Q(x)}} Q(x)^{k-1} + (-1)^k \sum_{\substack{Q \in -\mathcal{A} \\ a<0<Q(x)}} Q(x)^{k-1}$$

where the summation is restricted to quadratic forms in one equivalence class $\mathcal{A} \subset \mathfrak{Q}_D$ which is an orbit in $\mathfrak{Q}_D$ under the action of $\mathrm{PSL}_2(\mathbb{Z})$, and

$$-\mathcal{A} = \{-Q \mid Q \in \mathcal{A}\}.$$

However, restricting to one class $\mathcal{A}$ does not allow for a generalization to odd k of one of important properties of $F_{k,D}(x)$ which is discussed in [21, Section 14]. Namely, one can define a constant $F_{k,0}$ such that for every x, for even $k \geq 2$, the generating function $F_{k,0} + \sum_D F_{k,D}(x) q^D$, where the sum is taken over all discriminants $D > 0$, is the q-expansion of a modular form of weight $k + 1/2$. The functions $F_{k,D}(x)$ are 1-periodic, and their average values are calculated by Zagier in [21, Section

8]. These are, up to a common multiple, q-expansion coefficients of H. Cohen's Eisenstein series $\mathcal{H}_k(\tau)$. In order to state the result of this calculation, we recall that

$$\mathcal{H}_k(\tau) = \zeta(1-2k) + \sum_{(-1)^k D>0} H(k,|D|)q^{|D|} \quad \text{with } q = \exp(2\pi i\tau) \text{ and } \Im(\tau) > 0 \text{ throughout.}$$

The summation runs over discriminants D such that $(-1)^k D > 0$, and $H(k,|D|)$ denote Cohen's numbers as defined in the previous section. These numbers are essentially the values at negative integers of Dirichlet L-function of the quadratic character associated with the field extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$.

The result of Zagier's calculation in [21, Section 8] can now be stated as the identity

$$\frac{\zeta(1-2k)}{\zeta(1-k)}\left(\frac{1}{2}\zeta(1-k) + \sum_{D>0}\int_0^1 F_{k,D}(x)dx\ q^D\right) = \frac{1}{2}\mathcal{H}_k(\tau) \tag{2.1}$$

which holds for even $k \geq 2$.

In this chapter, we present a generalization of $F_{k,D}(x)$ which allows us to produce an exact analogue of (2.1) for odd k.

Let D be any discriminant, d be a fundamental discriminant such that $\Delta := Dd > 0$. For a quadratic form $Q = ax^2 + bx + c = [a,b,c]$ with integer coefficients and of discriminant

$$b^2 - 4ac = \Delta,$$

the value of the genus character $\chi_d(Q)$ is defined (cf. [7]) by

$$\chi_d(Q) = \begin{cases} 0 & \text{if } (a,b,c,d) > 1, \\ \left(\frac{d}{r}\right) & \text{if } (a,b,c,d) = 1, \end{cases}$$

where r is an integer represented by Q (i.e., there exists an integer n such that $an^2 + bn + c = r$) with $(r,d) = 1$. Such an r exists and the value of $\left(\frac{d}{r}\right)$ is independent of the choice of r.

We now assume that $k > 1$ is an integer, and

$$\operatorname{sign} d = \operatorname{sign} D = (-1)^k.$$

We define

$$F_{k,D,d}(x) := \sum_{\substack{Q\in\mathfrak{Q}_\Delta \\ a<0<Q(x)}} \chi_d(Q)Q(x)^{k-1}.$$

Note that our $F_{k,D,d}(x)$ generalizes Zagier's $F_{k,D}(x)$ directly. Namely, for even $k > 1$, we have

$$F_{k,D,1}(x) = F_{k,D}(x).$$

In section 2.2, we will show some basic properties of our functions $F_{k,D,d}(x)$, including 1-periodicity and continuity for $k > 1$, using the same argument as in [21], and thus their average values make sense. The main result of this chapter is the following generalization of (2.1).

Theorem 2.1. *For an integer $k > 1$, and a fundamental discriminant d such that* $\operatorname{sign} d = (-1)^k$,

$$\frac{\zeta(1-2k)}{H(k,|d|)}\left(\frac{1}{2}H(k,|d|) + \sum_{(-1)^k D>0} \int_0^1 F_{k,D,d}(x)dx\ q^{|D|}\right) = \frac{1}{2}\mathcal{H}_k(\tau).$$

It is quite natural to ask about the boundary case $k = 1$. It follows from [9] that $F_{1,D,d}(x)$ is defined if and only if x is rational, so no averaging is possible. At the same time, the series $\mathcal{H}_1$ is not modular (see [2, 19]). Thus, there is no direct analogue for Theorem 2.1 for $k = 1$. We prove that $F_{1,D,d}(x)$ is zero in the following theorem.

Theorem 2.2. *For a fundamental discriminant $d < 0$ and a discriminant $D < 0$ with Dd being non-square, and $x \in \mathbb{Q}$, we have that*

$$F_{1,D,d}(x) = 0.$$

The proof of Theorem 2.1 is presented in Section 2.3. Equality of constant terms of q-series in Theorem 2.1 follows directly from the definition of Cohen's numbers $H(k, N)$ in [2]. Thus Theorem 2.1 is equivalent to the term-by-term identity

$$\int_0^1 F_{k,D,d}(x)dx = \frac{H(k,|D|)H(k,|d|)}{2\zeta(1-2k)}, \tag{2.2}$$

and that is what we prove in Section 2.3. This proof depends on two technical propositions (Proposition 2.7 and 2.8 in Section 2.4) which claim a decomposition of a certain Dirichlet series into an Euler product, and calculate its Euler factors. The proofs of these propositions are presented in Section 2.4 of the chapter.

The value of the the genus character $\chi_d(Q) = \chi_d(\mathcal{A})$ depends only on the class $\mathcal{A} \in \mathfrak{Q}_\Delta$ such that $Q \in \mathcal{A}$, not on the individual form Q (see [7] for details). It follows that

$$F_{k,D,d}(x) = \sum_{\mathcal{A}} \chi_d(\mathcal{A}) F^*_{k,\mathcal{A}}(x), \tag{2.3}$$

where the sum is taken over all classes $\mathcal{A}$ of quadratic forms of discriminant Δ, and

$$F^*_{k,\mathcal{A}}(x) = \sum_{\substack{Q\in\mathcal{A}\\ a<0<Q(x)}} Q(x)^{k-1}.$$

The functions $F^*_{k,\mathcal{A}}(x)$ are introduced and briefly discussed in [21, Section 9]. In particular, since $F^*_{k,\mathcal{A}}(x)$ are periodic functions with period 1, so are our $F_{k,D,d}(x)$, and the integrals in the left of (2.2) may be interpreted as average values of these functions.

In Section 2.5, we address the case when $k = 1$.

2.2 Basic Properties of $F_{k,D,d}(x)$

First of all, we want to explain that the function $F_{k,D,d}(x)$ is well-defined for any integer $k > 1$. Then we will talk about several properties of $F_{k,D,d}(x)$.

We will quote the following properties (see [7, Proposition 1]) of the genus character that we will use in this chapter.

Proposition 2.3. *Let D be a discriminant and d be a fundamental discriminant with $\Delta = Dd$. Let $Q = [a, b, c] \in \mathfrak{Q}_\Delta$. Denote χ_d the genus character on $\mathfrak{Q}_\Delta$. Then*
(1) (Multiplicativity)

$$\chi_d([a, b, c]) = \chi_d([a_1, b, ca_2])\chi_d([a_2, b, ca_1]) \text{ if } a = a_1a_2 \text{ and } (a_1, a_2) = 1. \tag{2.4}$$

(2) (Invariance under the Fricke involution):

$$\chi_d([a, b, c]) = \chi_d([c, -b, a]). \tag{2.5}$$

(3) (Explicit formula)

$$\chi_d([a, b, c]) = \left(\frac{d_1}{a}\right)\left(\frac{d_2}{c}\right) \tag{2.6}$$

for any splitting $d = d_1d_2$ of d into discriminants (necessarily fundamental and coprime) and $(d_1, a) = (d_2, c) = 1$.

From the third property above, if $(a, b, c, d) = 1$, we can derive

$$\chi_d([a, -b, c]) = \left(\frac{1}{a}\right)\left(\frac{d}{c}\right) = \chi_d([a, b, c]), \tag{2.7}$$

and

$$\begin{aligned}\chi_d([-a,-b,-c]) &= \left(\frac{1}{-a}\right)\left(\frac{d}{-c}\right)\\ &= \left(\frac{1}{a}\right)\left(\frac{d}{c}\right)\left(\frac{d}{-1}\right)\\ &= \left(\frac{d}{-1}\right)\chi_d([a,b,c])\\ &= \begin{cases}\chi_d([a,b,c]) & \text{if } d>0,\\ -\chi_d([a,b,c]) & \text{if } d<0.\end{cases} \end{aligned} \tag{2.8}$$

Throughout the chapter, denote $\Delta = Dd$. We know that $\sum_{\substack{Q\in\mathfrak{Q}_\Delta\\ a<0<Q(x)}} \chi_d(Q)Q(x)^{k-1}$ is a finite sum if and only if $x \in \mathbb{Q}$ (see [9]). Thus, $F_{k,D,d}(x)$ is well-defined for rational x. We consider

$$\sum_{\substack{Q\in\mathfrak{Q}_\Delta\\ a<0<Q(x)}} |\chi_d(Q)Q(x)^{k-1}| \leq \sum_{\substack{Q\in\mathfrak{Q}_\Delta\\ a<0<Q(x)}} Q(x)^{k-1} = F_{k,\Delta}(x).$$

We know that $F_{k,\Delta}(x)$ converges for even k as shown in [21], but the same reasoning works for odd k as well. Thus, $F_{k,D,d}(x)$ converges for all $x \in \mathbb{R}$ for any $k > 1$.

In fact, our function $F_{k,D,d}(x)$ is continuous. With the same reasoning in [21], the sum $\sum_{\substack{Q\in\mathfrak{Q}_\Delta\\ a<0<Q(x)}} \chi_d(Q)Q(x)^{k-1}$ converges uniformly for all x for $k > 2$. For $k = 2$, we know that $F_{2,D,d}(x)$ is a linear combination of $F_{2,\mathcal{A}_i}(x)$ where $\mathcal{A}_i$ are equivalence classes of $\mathfrak{Q}_\Delta$ under the action of $PSL_2(\mathbb{Z})$. Since $F_{2,\mathcal{A}_i}(x)$ are constant functions, $F_{2,D,d}(x)$ is a constant function which is continuous.

Note that in our proofs, we will use the following equivalent sum for $F_{k,D,d}(x)$,

$$F_{k,D,d}(x) = \sum_{\substack{Q\in\mathfrak{Q}_\Delta\\ a<0<Q(x)}} \chi_d(Q)Q(x)^{k-1} = \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=\Delta\\ a<0}} \chi_d(Q)[\max(0, ax^2+bx+c)]^{k-1}.$$

Although we mentioned that $F_{k,D,d}(x)$ is periodic as a linear combination of periodic functions $F_{2,\mathcal{A}_i}(x)$, we will give a direct proof below.

Proposition 2.4. *For any integer $k > 1$, let D be a discriminant and d be a fundamental discriminant with $(-1)^k D > 0$ and $(-1)^k d > 0$. Then $F_{k,D,d}(x)$ is periodic with period 1.*

Proof. Consider

$$\begin{aligned} F_{k,D,d}(x+1) &= \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=\Delta \\ a<0}} \chi_d(Q)[\max(0, a(x+1)^2+b(x+1)+c)]^{k-1} \\ &= \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=\Delta \\ a<0}} \chi_d(Q)[\max(0, ax^2+(2a+b)x+(a+b+c))]^{k-1}. \end{aligned}$$

Let $A=a$, $B=2a+b$ and $C=a+b+c$. Then $B^2-4AC=(2a+b)^2-4a(a+b+c)=b^2-4ac$. Also, $\chi_d([a,b,c])=\chi_d([A,B,C])$ because χ_d is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$. Thus,

$$F_{k,D,d}(x+1) = \sum_{\substack{Q=[A,B,C]\in\mathbb{Z}^3 \\ B^2-4AC=\Delta \\ A<0}} \chi_d(Q)[\max(0, Ax^2+Bx+C)]^{k-1} = F_{k,D,d}(x)$$

as required. □

As an analogue of [21, Theorem 3], we will prove the following theorem.

Theorem 2.5. *Let k be a positive integer. Let D be a discriminant and d be a fundamental discriminant such that $(-1)^k D>0$ and $(-1)^k d>0$. Suppose $\Delta=Dd$ is not a perfect square. The function $F_{k,D,d}:\mathbb{R}\to\mathbb{R}$ defined by*

$$F_{k,D,d}(x) := \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ a<0}} \chi_d(Q)[\max(0, ax^2+bx+c)]^{k-1}$$

is a linear combination, with coefficients depending on D, d and k, of a finite collection of functions depending only on k.

Proof. Consider

$$\begin{aligned} &x^{2k-2}F_{k,D,d}\left(\frac{1}{x}\right) - F_{k,D,d}(x) \\ =&x^{2k-2}\sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ a<0}} \chi_d(Q)\left[\max\left(0, a\left(\frac{1}{x}\right)^2+b\left(\frac{1}{x}\right)+c\right)\right]^{k-1} - \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ a<0}} \chi_d(Q)[\max(0, ax^2+bx+c)]^{k-1} \\ =& \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ a<0}} \chi_d(Q)[\max(0, a+bx+cx^2)]^{k-1} - \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ a<0}} \chi_d(Q)[\max(0, ax^2+bx+c)]^{k-1} \end{aligned}$$

$$= \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ c<0}} \chi_d([c,b,a])[\max(0,ax^2+bx+c)]^{k-1} - \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ a<0}} \chi_d([a,b,c])[\max(0,ax^2+bx+c)]^{k-1}$$

$$= \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ c<0}} \chi_d([a,-b,c])[\max(0,ax^2+bx+c)]^{k-1} - \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ a<0}} \chi_d([a,b,c])[\max(0,ax^2+bx+c)]^{k-1}$$

$$= \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ c<0}} \chi_d([a,b,c])[\max(0,ax^2+bx+c)]^{k-1} - \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ a<0}} \chi_d([a,b,c])[\max(0,ax^2+bx+c)]^{k-1}$$

$$= \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ c<0<a}} \chi_d([a,b,c])[\max(0,ax^2+bx+c)]^{k-1} - \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ a<0<c}} \chi_d([a,b,c])[\max(0,ax^2+bx+c)]^{k-1}$$

(the terms with a and c both negative in the two sums cancel;

also note that ac can never vanish since Dd is not a square.)

$$= \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ a>0>c}} \chi_d([a,b,c])[\max(0,ax^2+bx+c)]^{k-1}$$

$$- \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ a<0<c}} \chi_d([a,b,c])[-\min(0,-ax^2-bx-c)]^{k-1}$$

$$= \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ a>0>c}} \chi_d([a,b,c])[\max(0,ax^2+bx+c)]^{k-1}$$

$$- (-1)^{k-1} \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ a<0<c}} \chi_d([a,b,c])[\min(0,-ax^2-bx-c)]^{k-1}$$

$$= \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ a>0>c}} \chi_d([a,b,c])[\max(0,ax^2+bx+c)]^{k-1}$$

$$(-1)^k \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ a<0<c}} (-1)^k\chi_d([-a,-b,-c])[\min(0,-ax^2-bx-c)]^{k-1}$$

$$= \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ a>0>c}} \chi_d([a,b,c])[\max(0,ax^2+bx+c)]^{k-1}$$

$$+ \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ a<0<c}} \chi_d([-a,-b,-c])[\min(0,-ax^2-bx-c)]^{k-1}$$

$$= \sum_{\substack{[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ a>0>c}} \chi_d([a,b,c])[\max(0,ax^2+bx+c)]^{k-1} + \sum_{\substack{[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ a>0>c}} \chi_d([a,b,c])[\min(0,ax^2+bx+c)]^{k-1}$$

$$= \sum_{\substack{[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ a>0>c}} \chi_d([a,b,c])(ax^2+bx+c)^{k-1}.$$

Define $P_{k,D,d}(x) := \sum_{\substack{[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ a>0>c}} \chi_d([a,b,c])(ax^2+bx+c)^{k-1}$. Now, $P_{k,D,d}(x)$ belongs to the (finite-dimensional) vector space $\mathfrak{M}^+_{2k-2}$ of all polynomials satisfying the functional equation $P(x+1) = P(x)+x^{2k-2}P\left(1+\frac{1}{x}\right)$. In fact, $\dim \mathfrak{M}^+_{2k-2} = \dim M_{2k}(\Gamma(1))$, the dimension of the space of modular forms of weight $2k$ on $\Gamma(1)$ (see [21]). Thus,

$$\dim \mathfrak{M}^+_{2k-2} = \begin{cases} \left[\frac{2k}{12}\right], & \text{if } 2k \equiv 2 \pmod{12}, \\ \left[\frac{2k}{12}\right]+1, & \text{otherwise} \end{cases}$$
$$= \begin{cases} \left[\frac{k}{6}\right], & \text{if } k \equiv 1 \pmod{6}, \\ \left[\frac{k}{6}\right]+1, & \text{otherwise.} \end{cases}$$

It follows that $F_{k,D,d}(x)$ is a linear combination of finitely many ($\leq \dim \mathfrak{M}^+_{2k-2}$) functions of x depending only on k, the coefficients being simply the coordinates of the polynomial $P_{k,D,d}(x)$ with respect to some fixed basis of a subspace of $\mathfrak{M}^+_{2k-2}$. In fact, consider $F_{k,D,d}(x)$ and the corresponding $P_{k,D,d}(x)$. Since any subspace of $\mathfrak{M}^+_{2k-2}$ is a finite dimensional space, there are finitely many values of D_i such that the corresponding functions $P_{k,D_i,d}$ span the subspace. Then $P_{k,D,d}(x) = a_1P_{k,D_1,d}(x) + \cdots + a_nP_{k,D_n,d}(x)$. Now consider the function $F(x) = F_{k,D,d}(x) - (a_1F_{k,D_1,d}(x)+\cdots+a_nF_{k,D_n,d}(x))$. We can see that $x^{2k-2}F\left(\frac{1}{x}\right)-F(x) = P_{k,D,d}(x)-(a_1P_{k,D_1,d}(x)+\cdots+a_nP_{k,D_n,d}(x)) = 0$. Thus, $x^{2k-2}F\left(\frac{1}{x}\right) = F(x)$. Also, $F(x+1) = F(x)$. Since $F(0) = F_{k,D,d}(0)-(a_1F_{k,D_1,d}(0)+\cdots+a_nF_{k,D_n,d}(0)) = -P_{k,D,d}(0)+(a_1P_{k,D_1,d}(0)+\cdots+a_nP_{k,D_n,d}(0)) = 0$, we can deduce that $F(x) = 0$ for all $x \in \mathbb{R}$. □

Now, we will give a direct proof that $F_{k,D,d}(x)$ is a constant function for small k.

Theorem 2.6. *For $k = 2,3,4,5$ and 7, $F_{k,D,d}(x)$ is a constant function for any discriminant D and fundamental discriminant d with Dd not a perfect square, $(-1)^kD > 0$ and $(-1)^kd > 0$.*

Proof. For $k = 2,4$, we know that $F_{k,D,d}(x)$ is constant because it is a linear combination of constant functions. Now, we will show that it is constant for $k = 3,5$ and 7 directly although Zagier claimed that for those odd k, $F_{k,\mathcal{A}}(x)$ are constant functions with $\mathcal{A}$ any equivalent class of quadratic forms with discriminant Dd.

First of all, note that $P_{k,D,d}(x)$ is a polynomial of degree $2k-2$. It is even and anti-invariant under $P_{k,D,d}(x) \mapsto x^{2k-2}P_{k,D,d}\left(\frac{1}{x}\right)$ since

$$x^{2k-2}P_{k,D,d}\left(\frac{1}{x}\right) = x^{2k-2}\left(\frac{1}{x^{2k-2}}F_{k,D,d}(x) - F_{k,D,d}\left(\frac{1}{x}\right)\right) = F_{k,D,d}(x) - x^{2k-2}F_{k,D,d}\left(\frac{1}{x}\right)$$
$$= -P_{k,D,d}(x).$$

Let $k=3$. We have

$$x^4F_{3,D,d}\left(\frac{1}{x}\right) - F_{3,D,d}(x) = P_{3,D,d}(x) = \sum_{\substack{[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ a>0>c}} \chi_d([a,b,c])(ax^2+bx+c)^2.$$

The right-hand side is a polynomial of degree 4, even, and anti-invariant under $P_{3,D,d}(x) \mapsto x^4P_{3,D,d}(\frac{1}{x})$, so it must have the form $P_{3,D,d}(x) = \alpha_{D,d}x^4 - \alpha_{D,d}$. Since $P_{3,D,d}(0) = F_{3,D,d}(0)$, we have $P_{3,D,d}(x) = F_{3,D,d}(0)x^4 - F_{3,D,d}(0)$. Now let $F^0_{3,D,d}(x) = F_{3,D,d}(x) - F_{3,D,d}(0)$. Thus, the function $F^0_{3,D,d}(x)$ vanishes for $x=0$ and satisfies the functional equations $F^0_{3,D,d}(x+1) = F^0_{3,D,d}(x)$ and $x^4F^0_{3,D,d}(1/x) = F^0_{3,D,d}(x)$. It follows that $F^0_{3,D,d}(x) = 0$ for all rational x. Since $F^0_{3,D,d}(x)$ is continuous, $F^0_{3,D,d}(x) = 0$ for all real x. This shows $F_{3,D,d}(x)$ is a constant function.

For $k=5$, we have $P_{5,D,d}(x) = \gamma_{D,d}x^8 + \gamma'_{D,d}x^6 - \gamma'_{D,d}x^2 - \gamma_{D,d}$ where $\gamma_{D,d} = F_{5,D,d}(0)$ and $\gamma'_{D,d}$ is some constant. Consider

$$\begin{aligned}
P_{5,D,d}(x+1) - P_{5,D,d}(x) =& (x+1)^8F_{5,D,d}\left(\frac{1}{x+1}\right) - F_{5,D,d}(x+1) - x^8F_{5,D,d}\left(\frac{1}{x}\right) + F_{5,D,d}(x)\\
=& (x+1)^8F_{5,D,d}\left(\frac{1}{x+1}\right) - x^8F_{5,D,d}\left(\frac{1}{x}\right)\\
=& (x+1)^8F_{5,D,d}\left(1-\frac{1}{x+1}\right) - x^8F_{5,D,d}\left(\frac{1}{x}+1\right)\\
=& x^8\left[\left(\frac{1}{x}+1\right)^8F_{5,D,d}\left(\frac{1}{\frac{1}{x}+1}\right) - F_{5,D,d}\left(\frac{1}{x}+1\right)\right]\\
=& x^8P_{5,D,d}\left(\frac{1}{x}+1\right).
\end{aligned}$$

Since x^8-1 satisfies $P(x+1) - P(x) = x^8P\left(\frac{1}{x}+1\right)$ but x^6-x^2 does not, we have $\gamma'_{D,d} = 0$ and $P_{5,D,d}(x) = \gamma_{D,d}x^8 - \gamma_{D,d}$. With the same argument, it follows that $F_{5,D,d}(x)$ is a constant function.

For $k=7$, $P_{7,D,d}(x) = \delta_{D,d}(x^{12}-1) + \delta'_{D,d}(x^{10}-x^2) - \delta''_{D,d}(x^8-x^4)$ where $\delta_{D,d} = F_{7,D,d}(0)$ and

$\delta'_{D,d}, \delta''_{D,d}$ are some constants. We have

$$P_{7,D,d}(x+1) - P_{7,D,d}(x) = x^{12} P_{7,D,d}\left(\frac{1}{x}+1\right)$$

Write $\delta' = \delta'_{D,d}$ and $\delta'' = \delta''_{D,d}$. Now substitute $P_{7,D,d}(x) = \delta_{D,d}(x^{12}-1) + \delta'_{D,d}(x^{10}-x^2) + \delta''_{D,d}(x^8 - x^4)$ into this equation; we get

$$\begin{aligned}(-8\delta' - 4\delta'')x^{11} + (-44\delta' - 22\delta'')x^{10} + (-110\delta' - 52\delta'')x^9 + (-165\delta' - 69\delta'')x^8 + \\ (-132\delta' - 48\delta'')x^7 + (132\delta' + 48\delta'')x^5 + (165\delta' + 69\delta'')x^4 + (110\delta' + 52\delta'')x^3 + \\ (44\delta' + 22\delta'')x^2 + (8\delta' + 4\delta'')x = 0.\end{aligned}$$

This implies $\delta' = \delta'' = 0$. Thus, $P_{7,D,d}(x) = \delta_{D,d}(x^{12}-1)$. With the same argument, $F_{7,D,d}(x)$ is constant. □

2.3 Proof of Theorem 2.1

In this section, we prove Theorem 2.1.

All we need is to prove (2.2). As in [21, Section 8], we have

$$\int_0^1 F_{k,D,d}(x)dx = \sum_{\substack{Q=[a,b,c]\in\mathfrak{Q}_{Dd}/\Gamma_\infty \\ a<0}} \chi_d(Q)\beta_k(Q),$$

where $\beta_k(Q) := \int_{-\infty}^{\infty}[\max(0,Q(x))]^{k-1}dx$. We evaluate this integral using the substitution $x = \frac{-b+t\sqrt{Dd}}{2a}$ with $dx = \frac{\sqrt{Dd}}{2a}dt$:

$$\begin{aligned}
\beta_k(Q) :&= \int_{-\infty}^{\infty}[\max(0,Q(x))]^{k-1}dx \\
&= \int_{\infty}^{-\infty}\left[\max\left(0, a\left(\frac{-b+t\sqrt{Dd}}{2a}\right)^2 + b\left(\frac{-b+t\sqrt{Dd}}{2a}\right)+c\right)\right]^{k-1}\frac{\sqrt{Dd}}{2a}dt \\
&= \int_{-\infty}^{\infty}\left[\max\left(0, \left(\frac{b^2-2bt\sqrt{Dd}+t^2Dd}{4a}+\frac{-b^2+bt\sqrt{Dd}}{2a}+c\right)\right)\right]^{k-1}\frac{\sqrt{Dd}}{2|a|}dt \\
&= \int_{-\infty}^{\infty}\left[\max\left(0, \left(\frac{b^2}{4a}-\frac{bt\sqrt{Dd}}{2a}+\frac{t^2Dd}{4a}+\frac{-b^2}{2a}+\frac{bt\sqrt{Dd}}{2a}+c\right)\right)\right]^{k-1}\frac{\sqrt{Dd}}{2|a|}dt \\
&= \int_{-\infty}^{\infty}\left[\max\left(0, \left(\frac{t^2Dd}{4a}+\frac{4ac-b^2}{4a}\right)\right)\right]^{k-1}\frac{\sqrt{Dd}}{2|a|}dt \\
&= \int_{-\infty}^{\infty}\left[\max\left(0, \left(\frac{(t^2-1)Dd}{4a}\right)\right)\right]^{k-1}\frac{\sqrt{Dd}}{2|a|}dt \\
&= \int_{-1}^{1}\left(\frac{(1-t^2)Dd}{4|a|}\right)^{k-1}\frac{\sqrt{Dd}}{2|a|}dt \\
&= \int_{-1}^{1}\frac{(1-t^2)^{k-1}(Dd)^{k-\frac{1}{2}}}{2^{2k-1}|a|^k}dt \\
&= \frac{(Dd)^{k-\frac{1}{2}}}{2^{2k-1}|a|^k}\int_{-1}^{1}(1-t^2)^{k-1}dt \\
&= (Dd)^{k-\frac{1}{2}}|a|^{-k}c_k \quad \text{with} \quad c_k := \frac{1}{2^{2k-1}}\int_{-1}^{1}(1-t^2)^{k-1}dt = \frac{1}{2^{2k-1}}\frac{\Gamma(k)\Gamma(\frac{1}{2})}{\Gamma(k+\frac{1}{2})}.
\end{aligned}$$

It follows that

$$\int_0^1 F_{k,D,d}(x)dx = c_k|Dd|^{k-1/2} \sum_{\substack{Q=[a,b,c]\in\mathfrak{Q}_{Dd}/\Gamma_\infty \\ a<0}} \frac{\chi_d(Q)}{|a|^k}$$
$$= c_k|Dd|^{k-1/2} \sum_{n=1}^{\infty} \left(\sum_{\substack{0\le b\le 2n-1 \\ b^2\equiv Dd \pmod{4n}}} \chi_d\left(\left[-n, b, \frac{Dd-b^2}{4n}\right]\right)\right) \frac{1}{n^k}.$$

Proposition 2.7. *Let $k>1$ be an integer. Let d be a fundamental discriminant and D be a discriminant such that $(-1)^k d > 0$ and $(-1)^k D > 0$. For a positive integer n, let*

$$N_{D,d}(n) := \sum_{\substack{0\le b\le 2n-1 \\ b^2\equiv Dd \pmod{4n}}} \chi_d\left(\left[-n, b, \frac{Dd-b^2}{4n}\right]\right).$$

The function $(-1)^k N_{D,d}\colon \mathbb{N}\to\mathbb{Z}$ is multiplicative.

We postpone a proof of Proposition 2.7 until Section 2.4, and continue with our proof of Theorem 2.1.

Proposition 2.7 allows us to write an Euler product expansion for the series $\sum_{n=1}^{\infty}(-1)^k N_{D,d}(n)n^{-k}$ with absolutely convergence, and we have that

$$\int_0^1 F_{k,D,d}(x)dx = c_k|Dd|^{k-1/2}\sum_{n=1}^{\infty}\frac{N_{D,d}(n)}{n^k}$$
$$= (-1)^k c_k|Dd|^{k-1/2}\sum_{n=1}^{\infty}\frac{(-1)^k N_{D,d}(n)}{n^k}$$
$$= (-1)^k c_k|Dd|^{k-1/2}\prod_p\sum_{n=0}^{\infty}\frac{(-1)^k N_{D,d}(p^n)}{p^{nk}}.$$

Our next proposition calculates the Euler factors in the above product.

Proposition 2.8. *Let p be a prime. Let $D = D_0 f^2$ with a fundamental discriminant D_0. Let $e\ge 0$ be the integer defined by $p^e || f$. Then*

$$\sum_{n=0}^{\infty}\frac{(-1)^k N_{D,d}(p^n)}{p^{nk}} = \frac{1-p^{-2k}}{\left(1-\left(\frac{D_0}{p}\right)p^{-k}\right)\left(1-\left(\frac{d}{p}\right)p^{-k}\right)}\frac{1}{(p^e)^{2k-1}}\left(\sigma_{2k-1}(p^e) - \left(\frac{D_0}{p}\right)p^{k-1}\sigma_{2k-1}(p^{e-1})\right), \tag{2.9}$$

where we adopt the usual convention $\sigma_{2k-1}(1/p)=0$.

We postpone a proof of Proposition 2.8 until Section 2.4, and continue with our proof of Theorem 2.1.

Assume that $D = D_0 f^2$ with a fundamental discriminant D_0, and let $f = \prod_{i=1}^m p_i^{e_i}$. An inductive argument on the number of prime factors of f allows us to conclude that

$$\frac{1}{f^{2k-1}} \sum_{r|f} \mu(r) \left(\frac{D_0}{r}\right) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) = \prod_{i=1}^m \frac{1}{(p_i^{e_i})^{2k-1}} \left(\sigma_{2k-1}(p_i^{e_i}) + \mu(p_i) \left(\frac{D_0}{p_i}\right) p_i^{k-1} \sigma_{2k-1}(p_i^{e_i-1})\right).$$

We take this equality into the account and use Proposition 2.8 to find that

$$\begin{aligned}
&\int_0^1 F_{k,D,d}(x)dx \\
=&(-1)^k c_k |Dd|^{k-1/2} \left(\prod_p \frac{1-p^{-2k}}{\left(1-\left(\frac{D_0}{p}\right)p^{-k}\right)\left(1-\left(\frac{d}{p}\right)p^{-k}\right)} \right) \frac{1}{f^{2k-1}} \sum_{r|f} \mu(r) \left(\frac{D_0}{r}\right) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
=&(-1)^k c_k |Dd|^{k-1/2} L_{D_0}(k) L_d(k) \frac{1}{\zeta(2k)} \frac{1}{f^{2k-1}} \sum_{r|f} \mu(r) \left(\frac{D_0}{r}\right) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
=&(-1)^k c_k |D_0 d|^{k-1/2} L_{D_0}(k) L_d(k) \frac{1}{\zeta(2k)} \sum_{r|f} \mu(r) \left(\frac{D_0}{r}\right) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right).
\end{aligned}$$

If k is even,

$$\begin{aligned}
\int_0^1 F_{k,D,d}(x)dx &= c_k |D_0 d|^{k-1/2} \frac{\zeta_{D_0}(k)}{\zeta(k)} \frac{\zeta_d(k)}{\zeta(k)} \frac{1}{\zeta(2k)} \sum_{r|f} \mu(r) \chi_{D_0}(r) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
&= \frac{c_k |D_0|^{k-1/2} \frac{\zeta_{D_0}(k)}{\zeta(2k)} \cdot c_k |d|^{k-1/2} \frac{\zeta_d(k)}{\zeta(2k)}}{c_k \frac{\zeta(k)^2}{\zeta(2k)}} \sum_{r|f} \mu(r) \chi_{D_0}(r) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
&= \frac{\frac{\zeta_{D_0}(1-k)}{2\zeta(1-2k)} \cdot \frac{\zeta_d(1-k)}{2\zeta(1-2k)}}{\frac{\zeta(1-k)^2}{2\zeta(1-2k)}} \sum_{r|f} \mu(r) \chi_{D_0}(r) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
&= \frac{\frac{\zeta_{D_0}(1-k)}{\zeta(1-k)} \cdot \frac{\zeta_d(1-k)}{\zeta(1-k)}}{2\zeta(1-2k)} \sum_{r|f} \mu(r) \chi_{D_0}(r) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
&= \frac{L_{D_0}(1-k) L_d(1-k)}{2\zeta(1-2k)} \sum_{r|f} \mu(r) \chi_{D_0}(r) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
&= \frac{H(k,|D_0|) H(k,|d|)}{2H(k,0)} \sum_{r|f} \mu(r) \chi_{D_0}(r) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
&= \frac{H(k,|D|) H(k,|d|)}{2H(k,0)}.
\end{aligned}$$

If k is odd,

$$\begin{aligned}
\int_0^1 F_{k,D,d}(x)dx &= (-1)^k c_k |D_0 d|^{k-1/2} L_{D_0}(k) L_d(k) \frac{1}{\zeta(2k)} \sum_{r|f} \mu(r)\chi_{D_0}(r) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
&= (-1)^k c_k |D_0 d|^{k-1/2} \frac{\pi^{k-\frac{1}{2}}\Gamma\left(1-\frac{k}{2}\right)}{|D_0|^{k-\frac{1}{2}}\Gamma\left(\frac{k+1}{2}\right)} \cdot \frac{\pi^{k-\frac{1}{2}}\Gamma\left(1-\frac{k}{2}\right)}{|d|^{k-\frac{1}{2}}\Gamma\left(\frac{k+1}{2}\right)} \cdot \frac{L(1-k,\chi_{D_0})L(1-k,\chi_d)}{\zeta(2k)} \\
&\quad \cdot \sum_{r|f} \mu(r)\chi_{D_0}(r) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
&= (-1)^k c_k \frac{\pi^{2k-1}\Gamma\left(1-\frac{k}{2}\right)^2}{\Gamma\left(\frac{k+1}{2}\right)^2} \cdot \frac{L(1-k,\chi_{D_0})L(1-k,\chi_d)}{\zeta(2k)} \cdot \sum_{r|f} \mu(r)\chi_{D_0}(r) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
&= \frac{(-1)^k \pi^{2k-1}}{2^{2k-1}} \cdot \frac{\Gamma(k)\Gamma\left(\frac{1}{2}\right)\Gamma\left(1-\frac{k}{2}\right)^2}{\Gamma\left(k+\frac{1}{2}\right)\Gamma\left(\frac{k+1}{2}\right)^2} \cdot \frac{\Gamma(k)}{\pi^{2k-\frac{1}{2}}\Gamma\left(\frac{1}{2}-k\right)\zeta(1-2k)} L(1-k,\chi_{D_0})L(1-k,\chi_d) \\
&\quad \cdot \sum_{r|f} \mu(r)\chi_{D_0}(r) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
&= \frac{(-1)^k}{2^{2k-1}} \cdot \frac{\Gamma(k)^2\Gamma\left(1-\frac{k}{2}\right)^2}{\Gamma\left(k+\frac{1}{2}\right)\Gamma\left(\frac{k+1}{2}\right)^2\Gamma\left(\frac{1}{2}-k\right)} \cdot \frac{L(1-k,\chi_{D_0})L(1-k,\chi_d)}{\zeta(1-2k)} \\
&\quad \cdot \sum_{r|f} \mu(r)\chi_{D_0}(r) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
&= \frac{(-1)^k}{2^{2k-1}} \cdot \frac{\Gamma(k)^2\Gamma\left(1-\frac{k}{2}\right)^2}{(-1)^k\pi\Gamma\left(\frac{k+1}{2}\right)^2} \cdot \frac{L(1-k,\chi_{D_0})L(1-k,\chi_d)}{\zeta(1-2k)} \cdot \sum_{r|f} \mu(r)\chi_{D_0}(r) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
&= \frac{1}{2^{2k-1}\pi} \cdot \frac{\Gamma\left(1-\frac{k}{2}\right)^2\Gamma\left(\frac{k}{2}\right)^2}{2^{2-2k}\pi} \cdot \frac{L(1-k,\chi_{D_0})L(1-k,\chi_d)}{\zeta(1-2k)} \cdot \sum_{r|f} \mu(r)\chi_{D_0}(r) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
&= \frac{1}{2\pi^2} \cdot \frac{\pi^2}{\sin^2\left(\frac{\pi k}{2}\right)} \frac{L(1-k,\chi_{D_0})L(1-k,\chi_d)}{\zeta(1-2k)} \cdot \sum_{r|f} \mu(r)\chi_{D_0}(r) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
&= \frac{L(1-k,\chi_{D_0})L(1-k,\chi_d)}{2\zeta(1-2k)} \cdot \sum_{r|f} \mu(r)\chi_{D_0}(r) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
&= \frac{H(k,|D_0|)H(k,|d|)}{2H(k,0)} \sum_{r|f} \mu(r)\chi_{D_0}(r) r^{k-1} \sigma_{2k-1}\left(\frac{f}{r}\right) \\
&= \frac{H(k,|D|)H(k,|d|)}{2H(k,0)}.
\end{aligned}$$

2.4 Proofs of Propositions 2.7 and 2.8

Proof of Proposition 2.7. Let n_1 and n_2 be two positive integers such that $(n_1, n_2) = 1$. We want to prove that

$$N_{D,d}(n_1 n_2) = N_{D,d}(n_1) N_{D,d}(n_2).$$

Without loss of generality, assume that n_2 is odd. Thus, $(n_2, 4) = 1$ and $(4n_1, n_2) = 1$.

We use our definition of $N_{D,d}(n)$ to transform these quantities. We obtain

$$\begin{aligned}
N_{D,d}(n_1 n_2) &= \sum_{\substack{0 \le b \le 2n_1 n_2 - 1 \\ b^2 \equiv Dd \pmod{4n_1 n_2}}} \chi_d\left(\left[-n_1 n_2, b, \frac{Dd - b^2}{4n_1 n_2}\right]\right) \\
&= \sum_{\substack{0 \le b \le 2n_1 n_2 - 1 \\ b^2 \equiv Dd \pmod{4n_1 n_2}}} \chi_d\left(\left[-n_1, b, \frac{Dd - b^2}{4n_1 n_2} \cdot n_2\right]\right) \chi_d\left(\left[n_2, b, \frac{Dd - b^2}{4n_1 n_2} \cdot (-n_1)\right]\right) \\
&= \sum_{\substack{0 \le b \le 2n_1 n_2 - 1 \\ b^2 \equiv Dd \pmod{4n_1 n_2}}} \chi_d\left(\left[-n_1, b, \frac{Dd - b^2}{4n_1}\right]\right) \chi_d\left(\left[n_2, b, -\frac{Dd - b^2}{4n_2}\right]\right) \\
&= (-1)^k \sum_{\substack{0 \le b \le 2n_1 n_2 - 1 \\ b^2 \equiv Dd \pmod{4n_1 n_2}}} \chi_d\left(\left[-n_1, b, \frac{Dd - b^2}{4n_1}\right]\right) \chi_d\left(\left[-n_2, b, \frac{Dd - b^2}{4n_2}\right]\right). \qquad (2.10)
\end{aligned}$$

Now consider

$$\begin{aligned}
N_{D,d}(n_1) N_{D,d}(n_2) &= \sum_{\substack{0 \le b_1 \le 2n_1 - 1 \\ b_1^2 \equiv Dd \pmod{4n_1}}} \chi_d\left(\left[-n_1, b_1, \frac{Dd - b_1^2}{4n_1}\right]\right) \sum_{\substack{0 \le b_2 \le 2n_2 - 1 \\ b_2^2 \equiv Dd \pmod{4n_2}}} \chi_d\left(\left[-n_2, b_2, \frac{Dd - b_2^2}{4n_2}\right]\right) \\
&= \sum_{\substack{0 \le b_1 \le 2n_1 - 1 \\ b_1^2 \equiv Dd \pmod{4n_1} \\ 0 \le b_2 \le 2n_2 - 1 \\ b_2^2 \equiv Dd \pmod{4n_2}}} \chi_d\left(\left[-n_1, b_1, \frac{Dd - b_1^2}{4n_1}\right]\right) \chi_d\left(\left[-n_2, b_2, \frac{Dd - b_2^2}{4n_2}\right]\right). \qquad (2.11)
\end{aligned}$$

Note that the sums (2.10) and (2.11) have same number of summands. Indeed, denote by $v(n)$ the number of solutions of $b^2 - Dd \equiv 0 \pmod{n}$. Then the number of summands in (2.10) is

$$\frac{1}{2} v(4n_1 n_2) = \frac{1}{2} v(4n_1) v(n_2)$$

while the number of summands in (2.11) is

$$\frac{1}{2} v(4n_1) \cdot \frac{1}{2} v(4n_2) = \frac{1}{2} v(4n_1) \cdot \frac{1}{2} v(4) v(n_2) = \frac{1}{2} v(4n_1) v(n_2).$$

We now establish a one-to-one correspondence between these sets of summands such that corresponding summands are equal.

Summands in (2.11) are numerated by pairs (b_1, b_2) of residues modulo $2n_1$ and $2n_2$ correspondingly (which satisfy additional congruence conditions modulo $4n_1$ and $4n_2$). The Chinese Remainder Theorem allows us to find B (unique modulo $4n_1n_2$) such that

$$B \equiv b_1 \pmod{4n_1} \quad \text{and } B \equiv b_2 \pmod{n_2}.$$

We now lift B to an integer, which we also denote by B such that $0 \leq B < 4n_1n_2$, and set

$$b = \begin{cases} B & \text{if } B < 2n_1n_2, \\ 4n_1n_2 - B & \text{if } B \geq 2n_1n_2. \end{cases}$$

It is easy to see that the above procedure establishes a one-to-one correspondence between the sets of summands in (2.10) and (2.11), and we now want to check that corresponding summands are equal.

Since $b \equiv \pm b_1 \pmod{4n_1}$, we set $b = \pm b_1 + 4n_1m = \pm b_1 + (2n_1)(2m)$ for some integer m and find that

$$\chi_d\left(\left[-n_1, b_1, \frac{Dd - b_1^2}{4n_1}\right]\right) = \chi_d\left(\left[-n_1, b, \frac{Dd - b^2}{4n_1}\right]\right).$$

Since $b \equiv \pm b_2 \pmod{n_2}$, we set $b = \pm b_2 + n_2m$ for some integer m. The congruence $b_2^2 \equiv Dd \pmod{4}$ implies $b_2 \equiv Dd \pmod{2}$. Similarly, $b^2 \equiv Dd \pmod{4}$ implies $b \equiv Dd \pmod{2}$ and $b \equiv b_2 \pmod{2}$. Since n_2 is odd, m must be even, $m = 2m'$. Thus, $b = \pm b_2 + n_2m = \pm b_2 + n_2(2m') = \pm b_2 + 2n_2(m')$. Now we have

$$\chi_d\left(\left[-n_2, b_2, \frac{Dd - b_2^2}{4n_2}\right]\right) = \chi_d\left(\left[-n_2, b, \frac{Dd - b^2}{4n_2}\right]\right).$$

It follows that

$$N_{D,d}(n_1n_2) = (-1)^k N_{D,d}(n_1)N_{D,d}(n_2),$$

therefore

$$(-1)^k N_{D,d}(n_1n_2) = [(-1)^k N_{D,d}(n_1)][(-1)^k N_{D,d}(n_2)]$$

as required. □

We now turn to the proof of Proposition 2.8. This proof varies slightly depending on whether the involved quantities are or are not divisible by p. Also, the case $p = 2$ has to be considered separately. In particular, we say that we are in **Case 1** if $p \nmid f$, and in **Case 2** if $p|f$. In each case, we consider the following sub-cases

(i) $p \nmid d$, $p \nmid D_0$

(ii) $p \nmid d$, $p | D_0$

(iii) $p | d$, $p \nmid D_0$

(iv) $p | d$, $p | D_0$,

and in every sub-case we will have part **(a)** if p is odd, and part **(b)** for $p = 2$.

2.4.1 Case 1(i)(a)

Proof of Proposition 2.8 in **Case 1(i)(a)**. Recall the assumptions: $p \nmid f$, $p \nmid d$ and $p \nmid D_0$ with p odd.

In case 1, since $p \nmid f$, we have $e = 0$. Thus, the identity (2.9) reads

$$\sum_{n=0}^{\infty} \frac{(-1)^k N_{D,d}(p^n)}{p^{nk}} = \frac{1 - p^{-2k}}{\left(1 - \left(\frac{D_0}{p}\right) p^{-k}\right)\left(1 - \left(\frac{d}{p}\right) p^{-k}\right)},$$

which is what we need to prove.

In all cases, the main part is to compute

$$N_{D,d}(p^n) = \sum_{\substack{0 \le b \le 2p^n - 1 \\ b^2 \equiv Dd \pmod{4p^n}}} \chi_d\left(\left[-p^n, b, \frac{Dd - b^2}{4p^n}\right]\right).$$

Once we know $N_{D,d}(p^n)$ for all $n \ge 1$, we can compute the series $\sum_{n=0}^{\infty} \frac{(-1)^k N_{D,d}(p^n)}{p^{nk}}$.

As long as $p \nmid d$, we can use the explicit formula (2.6) for the genus character to get

$$\chi_d([-p^n, b, c]) = \left(\frac{d}{-p^n}\right)\left(\frac{1}{c}\right) = \left(\frac{d}{-p^n}\right).$$

We thus have that

$$N_{D,d}(p^n) = \sum_{\substack{0 \le b \le 2p^n - 1 \\ b^2 \equiv Dd \pmod{4p^n}}} \chi_d\left(\left[-p^n, b, \frac{Dd - b^2}{4p^n}\right]\right) = \left(\frac{d}{-p^n}\right) \sum_{\substack{0 \le b \le 2p^n - 1 \\ b^2 \equiv Dd \pmod{4p^n}}} 1.$$

We make use of notation (cf. [21, Section 8])

$$N_\Delta(n) = \sum_{\substack{0 \le b \le 2n - 1 \\ b^2 \equiv \Delta \pmod{4n}}} 1$$

to obtain

$$\begin{aligned}\sum_{n=0}^{\infty}\frac{(-1)^k N_{D,d}(p^n)}{p^{nk}} &= \sum_{n=0}^{\infty}\frac{(-1)^k\left(\frac{d}{-p^n}\right)N_{Dd}(p^n)}{p^{nk}}\\ &= \sum_{n=0}^{\infty}\frac{(-1)^k\left(\frac{d}{-1}\right)\left(\frac{d}{p^n}\right)N_{Dd}(p^n)}{p^{nk}}\\ &= \sum_{n=0}^{\infty}\frac{\left(\frac{d}{p}\right)^n N_{Dd}(p^n)}{p^{nk}}. \end{aligned} \tag{2.12}$$

Let $v(n)$ be the number of solutions of $f(b) = b^2 - Dd \equiv 0 \pmod{n}$. Since p is odd,

$$N_{Dd}(p^n) = \frac{1}{2}\cdot v(4p^n) = \frac{1}{2}\cdot v(4)\cdot v(p^n) = \frac{1}{2}\cdot 2\cdot v(p^n) = v(p^n).$$

If $\left(\frac{d}{p}\right) \neq \left(\frac{D}{p}\right) = \left(\frac{D_0}{p}\right)$, then $\left(\frac{Dd}{p}\right) = -1$, i.e., Dd is a quadratic non-residue modulo p. Therefore $v(p) = N_{Dd}(p) = 0$. That implies $N_{Dd}(p^n) = v(p^n) = 0$ for $n \geq 1$, and

$$\sum_{n=0}^{\infty}\frac{(-1)^k N_{D,d}(p^n)}{p^{nk}} = 1 = \frac{(1+p^{-k})(1-p^{-k})}{\left(1-\left(\frac{D_0}{p}\right)p^{-k}\right)\left(1-\left(\frac{d}{p}\right)p^{-k}\right)}$$

as required.

If $\left(\frac{d}{p}\right) = \left(\frac{D}{p}\right)$, then $\left(\frac{Dd}{p}\right) = 1$ and Dd is a quadratic residue modulo p. Thus, the equation $f(b) = b^2 - Dd \equiv 0 \pmod{p}$ has two solutions and we label them $\{\pm b_1\}$. Then $v(p) = N_{Dd}(p) = 2$. Since $f'(b) = 2b$, and $f'(\pm b_1) = \pm 2b_1 \not\equiv 0 \pmod{p}$, by Hensel's lemma (Theorem 1.7(a)) we have $N_{Dd}(p^n) = v(p^n) = 2$ for $n \geq 1$. Thus, we get

$$\sum_{n=0}^{\infty}\frac{(-1)^k N_{D,d}(p^n)}{p^{nk}} = \sum_{n=0}^{\infty}\frac{\left(\frac{d}{p}\right)^n N_{Dd}(p^n)}{p^{nk}} = 1 + \frac{\left(\frac{d}{p}\right)\cdot 2}{p^k} + \frac{\left(\frac{d}{p^2}\right)\cdot 2}{p^{2k}} + \frac{\left(\frac{d}{p^3}\right)\cdot 2}{p^{3k}} + \cdots$$

which is a geometric series and transforms to

$$\begin{aligned} 1 + \frac{2\left(\frac{d}{p}\right)p^{-k}}{1-\left(\frac{d}{p}\right)p^{-k}} = \frac{1+\left(\frac{d}{p}\right)p^{-k}}{1-\left(\frac{d}{p}\right)p^{-k}} &= \frac{\left(1+\left(\frac{d}{p}\right)p^{-k}\right)\left(1-\left(\frac{d}{p}\right)p^{-k}\right)}{\left(1-\left(\frac{d}{p}\right)p^{-k}\right)\left(1-\left(\frac{d}{p}\right)p^{-k}\right)}\\ &= \frac{(1+p^{-k})(1-p^{-k})}{\left(1-\left(\frac{D_0}{p}\right)p^{-k}\right)\left(1-\left(\frac{d}{p}\right)p^{-k}\right)}. \end{aligned}$$

as required. □

2.4.2 Case 1(i)(b)

Proof of Proposition 2.8 in **Case 1(i)(b)**. Recall the assumptions: $p \nmid f$, $p \nmid d$ and $p \nmid D_0$ with $p = 2$.

As the previous part of the sub-case, we have the equation (2.12)

$$\sum_{n=0}^{\infty} \frac{(-1)^k N_{D,d}(2^n)}{2^{nk}} = \sum_{n=0}^{\infty} \frac{\left(\frac{d}{2}\right)^n N_{Dd}(2^n)}{2^{nk}}.$$

Note that $N_{Dd}(2^n) = \frac{1}{2} \cdot v(2^{n+2})$. We will first find $N_{Dd}(2) = v(8)$. Since $D, d \equiv 1 \pmod 4$, we have $D, d \equiv 1$ or $5 \pmod 8$. Note that the equation $b^2 - Dd \equiv 0 \pmod 8$ only has solutions when $d \equiv D \pmod 8$. Thus, if $d \not\equiv D \pmod 8$, we have $N_{Dd}(2) = 0$ and $N_{Dd}(2^n) = 0$ for $n \geq 1$. Then, we have

$$\sum_{n=0}^{\infty} \frac{(-1)^k N_{D,d}(2^n)}{2^{nk}} = 1 = \frac{(1+2^{-k})(1-2^{-k})}{\left(1 - \left(\frac{D_0}{2}\right) 2^{-k}\right)\left(1 - \left(\frac{d}{2}\right) 2^{-k}\right)}$$

because $\left(\frac{d}{2}\right) \neq \left(\frac{D_0}{2}\right)$. Now, if $d \equiv D \pmod 8$, we have $Dd \equiv 1 \pmod 8$. That means $b^2 \equiv Dd \pmod 8$ has 4 solutions, $\{1, 3, 5, 7\} = \{\pm 1, \pm 5\}$. Thus, $v(8) = 4$ and $N_{Dd}(2) = 2$. Now, we claim that $v(2^{n+2}) = 4$ for $n \geq 1$, i.e., $b^2 \equiv Dd \pmod{2^m}$ has 4 solutions for $m \geq 3$ where $m = n+2$.

We show this by induction. We have already shown the first case when $m = 3$. Suppose $\{\pm b_1, \pm b_2\}$ is the solution set for $f(b) = b^2 - Dd \equiv 0 \pmod{2^m}$ with $2 \nmid b_1, b_2$ and $b_2 = b_1 + 2^{m-1}$. Since $f'(b) = 2b \equiv 0 \pmod 2$, we will check which solution satisfies the equation $b^2 - Dd \equiv 0 \pmod{2^{m+1}}$.

We know that $b_i^2 - Dd \equiv 0 \pmod{2^m}$ with $i \in \{1, 2\}$, thus $b_i^2 - Dd \equiv 0$ or $2^m \pmod{2^{m+1}}$. Suppose $b_1^2 - Dd \equiv b_2^2 - Dd \pmod{2^{m+1}}$. Then,

$$\begin{aligned}
& b_1^2 \equiv b_2^2 \pmod{2^{m+1}} \\
\iff & b_1^2 - b_2^2 \equiv 0 \pmod{2^{m+1}} \\
\iff & (b_1 + b_2)(b_1 - b_2) \equiv 0 \pmod{2^m + 1} \\
\iff & (b_1 + b_1 + 2^{m-1})(-2^{m-1}) \equiv 0 \pmod{2^{m+1}} \\
\iff & 2b_1 + 2^{m-1} \equiv 0 \pmod{2^2} \\
\iff & 2b_1 \equiv 0 \pmod{2^2} \\
\iff & b_1 \equiv 0 \pmod 2
\end{aligned}$$

which is a contradiction.

Thus, we have either $b_1^2 - Dd \equiv 0 \pmod{2^{m+1}}$ or $b_2^2 - Dd \equiv 0 \pmod{2^{m+1}}$ but not both. By Theorem 1.7(b), only two solutions are lifted, each in two distinct ways. This proves $v(2^{n+2}) = 4$

for $n \geq 1$ and thus $N_{Dd}(2^n) = 2$ for $n \geq 1$. Now, we have

$$\begin{aligned}
\sum_{n=0}^{\infty} \frac{(-1)^k N_{D,d}(2^n)}{p^{nk}} &= \sum_{n=0}^{\infty} \frac{\left(\frac{d}{2^n}\right) N_{Dd}(2^n)}{p^{nk}} \\
&= 1 + \frac{\left(\frac{d}{2}\right) \cdot 2}{2^k} + \frac{\left(\frac{d}{2}\right)^2 \cdot 2}{2^{2k}} + \frac{\left(\frac{d}{2}\right)^3 \cdot 2}{2^{3k}} + \cdots \\
&= \frac{(1+2^{-k})(1-2^{-k})}{\left(1 - \left(\frac{D_0}{2}\right) \cdot 2^{-k}\right)\left(1 - \left(\frac{d}{2}\right) \cdot 2^{-k}\right)}
\end{aligned}$$

as required. □

2.4.3 Case 1(ii) and 1(iii)

Proof of Proposition 2.8 in **Case 1(ii)(a)**. Recall the assumptions: $p \nmid f$, $p \nmid d$ and $p | D_0$ with p odd.

From the equation (2.12), we have

$$\sum_{n=0}^{\infty} \frac{(-1)^k N_{D,d}(p^n)}{p^{nk}} = \sum_{n=0}^{\infty} \frac{\left(\frac{d}{p}\right)^n N_{Dd}(p^n)}{p^{nk}}.$$

We first compute $N_{Dd}(p) = v(p)$. The equation $f(b) = b^2 - Dd \equiv 0 \pmod{p}$ has only one solution which is $b = 0$, so $N_{Dd}(p) = 1$. Now, $f(0) = -Dd \not\equiv 0 \pmod{p^2}$ because D_0 is a fundamental discriminant. Therefore, by Theorem 1.7, 0 cannot be lifted. The equation $b^2 - Dd \equiv 0 \pmod{p})^2$ has no solution and $N_{Dd}(p^2) = v(p^2) = 0$. This implies $N_{Dd}(p^n) = v(p^n) = 0$ for $n \geq 2$. We have

$$\begin{aligned}
\sum_{n=0}^{\infty} \frac{(-1)^k N_{D,d}(p^n)}{p^{nk}} = \sum_{n=0}^{\infty} \frac{\left(\frac{d}{p}\right)^n N_{Dd}(p^n)}{p^{nk}} &= 1 + \left(\frac{d}{p}\right) p^{-k} \\
&= \frac{\left(1 + \left(\frac{d}{p}\right) p^{-k}\right)\left(1 - \left(\frac{d}{p}\right) p^{-k}\right)}{1 - \left(\frac{d}{p}\right) p^{-k}} \\
&= \frac{(1+p^{-k})(1-p^{-k})}{\left(1 - \left(\frac{D_0}{p}\right) p^{-k}\right)\left(1 - \left(\frac{d}{p}\right) p^{-k}\right)}
\end{aligned}$$

because $\left(\dfrac{D_0}{p}\right) = 0$. □

Proof of Proposition 2.8 in **Case 1(ii)(b)**. Recall the assumptions: $p \nmid f$, $p \nmid d$ and $p|D_0$ with $p = 2$.

We will start with computing $N_{Dd}(2) = \frac{1}{2}v(8)$. Since $2|D_0$, it implies $D_0 = 4m$ where $m \equiv 2$ or $3 \pmod 4$ and m squarefree.

Assume $m \equiv 2 \pmod 4$. Then $D_0 \equiv 0 \pmod 8$ and $Dd \equiv 0 \pmod 8$. Thus, the equation $f(b) = b^2 - Dd \equiv 0 \pmod 8$ has only two solutions, namely $b = 0$ and $b = 4$. We have $v(8) = 2$ and $N_{Dd}(2) = 1$. Now consider the equation $b^2 - Dd \equiv 0 \pmod{16}$. We have $f'(b) = 2b \equiv 0 \pmod 2$ for any b. Note that $f(0) = -Dd = -4mf^2d \not\equiv 0 \pmod{16}$ since f and d are odd. Thus, by Theorem 1.7, the solution 0 cannot be lifted. On the other hand, $f(4) = 16 - Dd \equiv -Dd \not\equiv 0 \pmod{16}$. Thus, 4 cannot be lifted neither. We have $v(16) = 0$ and $N_{Dd}(4) = 0$. This implies $v(2^{n+2}) = 0$ and $N_{Dd}(2^n) = 0$ for $n \geq 2$.

Assume $m \equiv 3 \pmod 4$. Then $Dd = 4mf^2d \equiv 4 \pmod 8$. Then the equation $f(b) = b^2 - Dd \equiv 0 \pmod 8$ has only two solutions, namely $b = 2$ and $b = 6$. We have $v(8) = 2$ and $N_{Dd}(2) = 1$. Now consider the equation $b^2 - Dd \equiv 0 \pmod{16}$. Note that $f(2) = 4 - Dd = 4 - 4mf^2d = 4(1 - mf^2d) \not\equiv 0 \pmod{16}$ since $mf^2d \equiv 3 \pmod 4$ and $1 - mf^2d \equiv 2 \pmod 4$. Thus, 2 cannot be lifted. On the other hand, $f(6) = 36 - Dd = 36 - 4mf^2d = 4(9 - mf^2d) \not\equiv 0 \pmod{16}$ since $9 - mf^2d \equiv 1 - mf^2d \equiv 2 \pmod 4$. Thus, 6 cannot be lifted neither. We have $v(16) = 0$ and $N_{Dd}(4) = 0$. This implies $v(2^{n+2}) = 0$ and $N_{Dd}(2^n) = 0$ for $n \geq 2$. Therefore, for both cases, we have

$$
\begin{aligned}
\sum_{n=0}^{\infty} \frac{(-1)^k N_{D,d}(p^n)}{p^{nk}} &= \sum_{n=0}^{\infty} \frac{\left(\frac{d}{p}\right)^n N_{Dd}(p^n)}{p^{nk}} \\
&= 1 + \left(\frac{d}{p}\right) p^{-k} \\
&= \frac{\left(1 + \left(\frac{d}{p}\right) p^{-k}\right)\left(1 - \left(\frac{d}{p}\right) p^{-k}\right)}{1 - \left(\frac{d}{p}\right) p^{-k}} \\
&= \frac{(1 + p^{-k})(1 - p^{-k})}{\left(1 - \left(\frac{D_0}{p}\right) p^{-k}\right)\left(1 - \left(\frac{d}{p}\right) p^{-k}\right)}
\end{aligned}
$$

because $\left(\dfrac{D_0}{p}\right) = 0.$ □

Case 1(iii): $p \nmid f$, $p|d$ and $p \nmid D_0$

In this case, we can switch the role of d and D_0 since $\chi_d = \chi_{D_0}$ on primitive quadratic functions (see [7]). Thus, it is the same as Case 1(ii).

2.4.4 Case 1(iv)(a)

Proof of Proposition 2.8 in **Case 1(iv)(a)**. Recall the assumptions: $p \nmid f$, $p|d$ and $p|D_0$ with p odd.

In this sub-case, since $p|d$ and $p|D_0$, we have to compute $N_{D,d}(p^n)$ explicitly and cannot simply count solutions of the equation $x^2 - Dd \equiv 0 \pmod{4p^n}$ like the previous 3 sub-cases.

We make the following claims and will prove them after:

I. $N_{D,d}(p) = 0$.

II. $N_{D,d}(p^2) = (-1)^{k+1}$.

III. $N_{D,d}(p^n) = 0$ for $n \geq 3$.

Thus, we have

$$\sum_{n=0}^{\infty} \frac{(-1)^k N_{D,d}(p^n)}{p^{nk}} = 1 - \frac{1}{p^{2k}} = 1 - p^{-2k} = (1+p^{-k})(1-p^{-k})$$
$$= \frac{(1+p^{-k})(1-p^{-k})}{\left(1 - \left(\frac{D_0}{p}\right)p^{-k}\right)\left(1 - \left(\frac{d}{p}\right)p^{-k}\right)}$$

since $\left(\frac{D_0}{p}\right) = \left(\frac{d}{p}\right) = 0$. □

Proof of Claim I. First, consider the equation $f(b) = b^2 - Dd \equiv 0 \pmod{p}$ which has only one solution $b = 0$ because $p|Dd$. On the other hand, $b^2 - Dd \equiv 0 \pmod 4$ always has two solutions. So $f(b) \equiv 0 \pmod{4p}$ has two solutions $\{m_1 p, m_2 p\}$ where $m_1 = 0$, $m_2 = 2$ or $m_1 = 1$, $m_2 = 3$. Now,

$$N_{D,d}(p) = \sum_{\substack{0 \leq b \leq 2p-1 \\ b^2 \equiv Dd \pmod{4p}}} \chi_d\left(\left[-p, b, \frac{Dd - b^2}{4p}\right]\right) = \chi_d\left(\left[-p, m_1 p, \frac{Dd - (m_1 p)^2}{4p}\right]\right) = 0$$

because $p^2 | Dd - (m_1 p)^2$ and thus $p | \frac{Dd - (m_1 p)^2}{4p}$. □

Proof of Claim II. We will first show the case when k is even.

We know that the only solution to $f(b) = b^2 - Dd \equiv 0 \pmod{p}$ is $b = 0$ and since $f'(0) = 0$, the solution $b = 0$ is lifted from p to p^2 in p distinct solutions. Thus, the equation $b^2 - Dd \equiv 0 \pmod{p^2}$ has the solution set $\{tp\}_{t=0}^{p-1}$. On the other hand, $b^2 - Dd \equiv 0 \pmod 4$ always has two solutions. Now, by Theorem 1.6, the equation $b^2 \equiv Dd \pmod{4p^2}$ will have $v(4)v(p^2) = 2p$ solutions and the solution set is $\{tp + m_t p^2, tp + (m_t + 2)p^2)\}_{t=0}^{p-1}$ where $m_{t,1} = 0$ or 1. Now, let $b_t = tp + m_{t,1}p^2$ and $c_t = \frac{Dd-(tp+m_{t,1}p^2)^2}{4p^2}$. Thus, we have

$$N_{D,d}(p^2) = \sum_{t=0}^{p-1} \chi_d([-p^2, b_t, c_t]).$$

Note that by the explicit formula (2.6),

$$\begin{aligned}
\chi_d([-p^2, b_t, c_t]) &= \begin{cases} \left(\frac{\frac{d}{p}}{-p^2}\right)\left(\frac{p}{c_t}\right) & \text{if } p \equiv 1 \pmod 4, \\ \left(\frac{\frac{d}{-p}}{-p^2}\right)\left(\frac{-p}{c_t}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases} \\
&\left(\text{since both } \frac{d}{p} \text{ and } p \text{ or both} \frac{d}{-p} \text{ and } -p \text{ are congruent to 1 (mod 4)}\right) \\
&= \begin{cases} \left(\frac{\frac{d}{p}}{-1}\right)\left(\frac{p}{c_t}\right) & \text{if } p \equiv 1 \pmod 4, \\ \left(\frac{\frac{d}{-p}}{-1}\right)\left(\frac{-p}{c_t}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases} \\
&= \begin{cases} \left(\frac{p}{c_t}\right) & \text{if } p \equiv 1 \pmod 4, \\ -\left(\frac{-p}{c_t}\right) & \text{if } p \equiv 3 \pmod 4. \end{cases}
\end{aligned}$$

If $p \equiv 1 \pmod 4$, by quadratic reciprocity, we have

$$\chi_d([-p^2, b_t, c_t]) = \left(\frac{p}{c_t}\right) = \left(\frac{c_t}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{c_t}{p}\right) = \left(\frac{-c_t}{p}\right).$$

Consider $p \equiv 3 \pmod 4$. If $c_t \geq 0$, by quadratic reciprocity, we have

$$\left(\frac{-p}{c_t}\right) = \left(\frac{c_t}{-p}\right) = \left(\frac{c_t}{p}\right)\left(\frac{c_t}{-1}\right) = \left(\frac{c_t}{p}\right).$$

If $c_t < 0$, by quadratic reciprocity, we have

$$\left(\frac{-p}{c_t}\right) = -\left(\frac{c_t}{-p}\right) = -\left(\frac{c_t}{-1}\right)\left(\frac{c_t}{p}\right) = \left(\frac{c_t}{p}\right).$$

Thus, for $p \equiv 3 \pmod 4$, we have

$$\chi_d([-p^2, b_t, c_t]) = -\left(\frac{c_t}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{c_t}{p}\right) = \left(\frac{-c_t}{p}\right).$$

Therefore, we have

$$N_{D,d}(p^2) = \sum_{t=0}^{p-1} \left(\frac{-c_t}{p}\right).$$

We have

$$c_t = \frac{Dd - (tp + m_t p^2)^2}{4p^2} = \frac{Dd - (t^2p^2 + 2tpm_tp^2 + m_t^2p^4)}{4p^2} = \frac{Dd - t^2p^2 - 2tm_tp^3 - m_t^2p^4}{4p^2}.$$

Thus,

$$\left(\frac{-c_t}{p}\right) = \left(\frac{\frac{t^2p^2+2tm_tp^3+m_t^2p^4-Dd}{4p^2}}{p}\right) = \left(\frac{t^2 + 2tm_tp + t^2p^2 - \frac{D}{p}\cdot\frac{d}{p}}{p}\right) = \left(\frac{t^2 - \frac{D}{p}\cdot\frac{d}{p}}{p}\right).$$

Note that $p \nmid \frac{D}{p}\frac{d}{p}$ and by Proposition 1.5, $\sum_{t=0}^{p-1}\left(\frac{t^2-\frac{D}{p}\cdot\frac{d}{p}}{p}\right) = -1$. Thus,

$$N_{D,d}(p^2) = t\sum_{t=0}^{p-1}\left(\frac{-c_t}{p}\right) = -1.$$

When k is odd, everything follows except we have

$$\begin{aligned} N_{D,d}(p^2) &= \begin{cases} \sum_{t=0}^{p-1} -\left(\frac{c_t}{p}\right) & \text{if } p \equiv 1 \pmod 4, \\ \sum_{t=0}^{p-1}\left(\frac{c_t}{p}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases} \\ &= -\sum_{t=0}^{p-1}\left(\frac{-c_t}{p}\right) \end{aligned}$$

because now $\left(\frac{\frac{d}{p}}{-p^2}\right) = -1$ if $p \equiv 1 \pmod 4$ while $\left(\frac{\frac{d}{p}}{-p^2}\right) = 1$ if $p \equiv 3 \pmod 4$. So, we have $N_{D,d}(p^2) = 1$ when k is odd. □

Proof of Claim III. Remember the claim is that $N_{D,d}(p^n) = 0$ for $n \geq 3$.

We have seen that $\{tp\}_{t=1}^{p}$ is the set of solutions for the equation $f(b) = b^2 - Dd \equiv 0 \pmod{p^2}$. Also, $f'(tp) = 2tp \equiv 0 \pmod p$ for any $t \in \{1, ..., p\}$. Then we have the following equivalent statements:

$$
\begin{aligned}
&\quad tp \text{ is lifted from } p^2 \text{ to } p^3 \text{ in } p \text{ different ways}\\
\iff &\quad (tp)^2 - Dd \equiv 0 \pmod{p^3}\\
\iff &\quad t^2p^2 - Dd \equiv 0 \pmod{p^3}\\
\iff &\quad t^2 - \frac{Dd}{p^2} \equiv 0 \pmod{p}\\
\iff &\quad \frac{Dd}{p^2} \equiv t^2 \pmod{p}\\
\iff &\quad \left(\frac{\frac{Dd}{p^2}}{p}\right) = 1.
\end{aligned}
$$

Thus, if $\left(\frac{\frac{Dd}{p^2}}{p}\right) \neq 1$, then there are no solutions for $b^2 - Dd \equiv 0 \pmod{p^3}$ and $N_{D,d}(p^3) = 0$. Thus, $N_{D,d}(p^n) = 0$ for all $n \geq 3$.

If $\left(\frac{\frac{Dd}{p^2}}{p}\right) = 1$, then two non-zero solutions from $b^2 - Dd \equiv 0 \pmod{p^2}$ will be lifted from p^2 to p^3. We will call them t_1p and $-t_1p$ with $1 \leq t_1 \leq p-1$. Then the solution set to the equation $b^2 - Dd \equiv 0 \pmod{p^3}$ will be $B_3 = \{\pm t_1p + tp^2\}_{t=0}^{p-1}$ which is equivalent to $B_3 = \{\pm(t_1p+tp^2)\}_{t=0}^{p-1}$. To see this, $B_3 = \{\pm t_1p+tp^2\}_{t=0}^{p-1} = \{t_1p+tp^2, -t_1p+tp^2\}_{t=0}^{p-1} = \{t_1p+tp^2, -t_1p+tp^2-p^3\}_{t=0}^{p-1} = \{t_1p+tp^2, -t_1p+(t-p)p^2\}_{t=0}^{p-1} = \{t_1p+tp^2, -t_1p-(p-t)p^2\}_{t=0}^{p-1} = \{t_1p+tp^2, -t_1p-tp^2\}_{t=0}^{p-1} = \{\pm(t_1p+tp^2)\}_{t=0}^{p-1}$. Another simple way to see this is if b' is a non-zero solution to $b^2 - Dd \equiv 0 \pmod{p^3}$, $-b'$ must be another solution. Thus, the equation $b^2 - Dd \equiv 0 \pmod{4p^3}$ will have $4p$ solutions since each element in B_3 gives two different solutions by adding different multiples of p^3. Similar to what we did, we can label them $\{b_i\}_{i=1}^{4p} = \{\pm(t_1p+tp^2+m_{t,1}p^3), \pm(t_1p+tp^2+m_{t,2}p^3)\}_{t=0}^{p-1}$. Let $c_i = \frac{b_i^2 - Dd}{4(-p^3)}$ and $c_{t,j} = \frac{b_{t,j}^2 - Dd}{4(-p^3)}$ where $b_{t,j} = t_1p + tp^2 + m_{t,j}p^3$ with $1 \leq j \leq 2$. Then, by the explicit formula (2.6) and quadratic reciprocity again, we have

$$
\begin{aligned}
N_{D,d}(p^3) = \frac{1}{2}\sum_{i=1}^{4p} \chi_d([-p^3, b_i, c_i]) &= \begin{cases} \frac{1}{2}\sum_{i=1}^{4p} \left(\frac{\frac{d}{p}}{-p^3}\right)\left(\frac{p}{c_i}\right) & \text{if } p \equiv 1 \pmod{4},\\ \frac{1}{2}\sum_{i=1}^{4p} \left(\frac{\frac{d}{-p}}{-p^3}\right)\left(\frac{-p}{c_i}\right) & \text{if } p \equiv 3 \pmod{4} \end{cases}\\
&= \begin{cases} \frac{1}{2}\left(\frac{\frac{d}{p}}{-p}\right)\sum_{t=1}^{4p} \left(\frac{c_i}{p}\right) & \text{if } p \equiv 1 \pmod{4},\\ \frac{1}{2}\left(\frac{\frac{d}{-p}}{-p}\right)\sum_{t=1}^{4p} \left(\frac{c_i}{p}\right) & \text{if } p \equiv 3 \pmod{4} \end{cases}\\
&= \frac{1}{2}\left(\frac{\frac{d}{p}}{p}\right)\sum_{t=1}^{4p}\left(\frac{c_i}{p}\right).
\end{aligned}
$$

Note that

$$\left(\frac{c_{t,j}}{p}\right) = \left(\frac{\frac{(t_1p+tp^2+m_{t,j}p^3)^2-Dd}{-4p^3}}{p}\right) = \left(\frac{\frac{(t_1p+tp^2+m_{t,j}p^3)^2-Dd}{-p^3}}{p}\right) = \left(\frac{\frac{t_1^2p^2+2t_1tp^3-Dd}{-p^3}}{p}\right) = \left(\frac{\frac{t_1^2p^2-Dd}{-p^3}-2t_1t}{p}\right).$$

Since $p \nmid 2t_1$, we have $\sum_{t=1}^{p}\left(\frac{c_{t,j}}{p}\right) = 0$. Therefore,

$$N_{D,d}(p^3) = \frac{1}{2}\left(\frac{\frac{d}{p}}{p}\right)\sum_{i=1}^{4p}\left(\frac{c_i}{p}\right) = \frac{1}{2}\left(\frac{\frac{d}{p}}{p}\right)\sum_{t=1}^{p}2\sum_{j=1}^{2}\left(\frac{c_{t,j}}{p}\right) = \left(\frac{\frac{d}{p}}{p}\right)\sum_{j=1}^{2}\sum_{t=1}^{p}\left(\frac{c_{t,j}}{p}\right) = 0.$$

Thus, $N_{D,d}(p^3) = 0$.

Recall that the set of solutions to the equation $b^2 - Dd \equiv 0 \pmod{p^3}$ is $B_3 = \{\pm(t_1p+tp^2)\}_{t=1}^{p}$. To find $N_{D,d}(p^4)$, we repeat the same process. By Theorem 1.7, we have the following equivalent statements:

$$\begin{aligned}
&\text{The solutions } \pm(t_1p+tp^2) \text{ can be lifted from } p^3 \text{ to } p^4 \text{ in } p \text{ different ways.}\\
\Longleftrightarrow&[\pm(t_1p+tp^2)]^2 - Dd \equiv 0 \pmod{p^4}\\
\Longleftrightarrow&(t_1p+tp^2)^2 - Dd \equiv 0 \pmod{p^4}\\
\Longleftrightarrow&(t_1p)^2 + 2t_1tp^3 - Dd \equiv 0 \pmod{p^4}\\
\Longleftrightarrow&2t_1t \equiv -\frac{(t_1p)^2 - Dd}{p^3} \pmod{p}.\\
\Longleftrightarrow&2t_1t \equiv \frac{\left(\frac{Dd}{p^2} - t_1^2\right)}{p} \pmod{p}.
\end{aligned} \tag{2.13}$$

We know that $\frac{\left(\frac{Dd}{p^2}-t_1^2\right)}{p}$ is an integer because $\frac{Dd}{p^2} \equiv t_1^2 \pmod{p}$. There is a unique t, say t_2, that satisfies the equation (2.13) since it is a linear equation (with $p \nmid 2t_1$). Thus, each of the two solutions $\pm(t_1p+t_2p^2)$ is lifted from p^3 to p^4 in p distinct ways and now the equation $b^2 - Dd \equiv 0 \pmod{p^4}$ has the solution set $B_4 = \{\pm(t_1p+t_2p^2)+tp^3\}_{t=0}^{p-1} = \{\pm(t_1p+t_2p^2+tp^3)\}_{t=0}^{p-1}$. Similarly,

$$\begin{aligned}
&\text{The solutions } \pm(t_1p+t_2p^2+tp^3) \text{ are lifted from } p^4 \text{ to } p^5 \text{ in } p \text{ different ways.}\\
\Longleftrightarrow&[\pm(t_1p+t_2p^2+tp^3)]^2 - Dd \equiv 0 \pmod{p^5}\\
\Longleftrightarrow&(t_1p+t_2p^2+tp^3)^2 - Dd \equiv 0 \pmod{p^5}\\
\Longleftrightarrow&(t_1p+t_2p^2)^2 + 2t_1tp^4 - Dd \equiv 0 \pmod{p^5}\\
\Longleftrightarrow&2t_1t \equiv -\frac{(t_1p+t_2p^2)^2 - Dd}{p^4} \pmod{p}.
\end{aligned} \tag{2.14}$$

From the equation (2.13), we know $\frac{(t_1p+t_2p^2)^2-Dd}{p^4}$ is an integer and thus there is a unique t, say t_3 that satisfies the equation (2.14) since it is a linear equation (with $p \nmid 2t_1$). Thus, the solutions $\pm(t_1p + t_2p^2 + t_3p^3)$ are lifted from p^4 to p^5 in p distinct ways and now the equation $b^2 - Dd \equiv 0 \pmod{p^5}$ has the solution set $B_5 = \{\pm(t_1p + t_2p^2 + t_3p^3 + tp^4)\}_{t=0}^{p-1}$.

By an induction process, we have the relation

$$\begin{aligned}&(t_1p + t_2p^2 + \cdots + t_{n-2}p^{n-2})^2 - Dd \equiv 0 \pmod{p^n}\\ \Longleftrightarrow &2t_1t_{n-2} \equiv -\frac{(t_1p + t_2p^2 + \cdots + t_{n-3}p^{n-3})^2 - Dd}{p^{n-1}} \pmod{p}.\end{aligned}$$

and the equation $b^2 - Dd \equiv 0 \pmod{p^n}$ with $n \geq 4$ have the solution set $B_n = \{\pm(t_1p + t_2p^2 + \cdots + t_{n-2}p^{n-2} + tp^{n-1})\}_{t=0}^{p-1}$ with $2p$ solutions. Then the equation $b^2 - Dd \equiv 0 \pmod{4p^n}$ will have $4p$ solutions $\{b_i\}_{i=1}^{4p} = \{\pm(t_1p + tp^2 + \cdots + t_{n-2}p^{n-2} + tp^{n-1} + m_{t,1}p^n), \pm(t_1p + tp^2 + \cdots + t_{n-2}p^{n-2} + tp^{n-1} + m_{t,2}p^n)\}$. Note that we abuse the notations here by using $\{b_i\}$, $m_{t,1}$ and $m_{t,2}$. Let $c_i = \frac{b_i^2-Dd}{4(-p^n)}$ and $c_{t,j} = \frac{b_{t,j}^2-Dd}{4(-p^n)}$ where $b_{t,j} = t_1p + tp^2 + \cdots + t_{n-2}p^{n-2} + tp^{n-1} + m_{t,j}p^n$ with $1 \leq j \leq 2$.

Then, by the explicit formula (2.6) and quadratic reciprocity again, we have

$$N_{D,d}(p^n) = \frac{1}{2}\sum_{t=1}^{4p} \chi_d([-p^n, b_i, c_i]) = \begin{cases} \frac{1}{2}\left(\frac{\frac{d}{p}}{-p^n}\right)\sum_{t=1}^{4p}\left(\frac{c_i}{p}\right) & \text{if } p \equiv 1 \pmod{4},\\ \frac{1}{2}\left(\frac{\frac{d}{-p}}{-p^n}\right)\sum_{t=1}^{4p}\left(\frac{c_i}{p}\right) & \text{if } p \equiv 3 \pmod{4}.\end{cases}$$

Note that

$$\begin{aligned}\left(\frac{c_{t,j}}{p}\right) &= \left(\frac{\frac{(t_1p+tp^2+\cdot t_{n-2}p^{n-2}+tp^{n-1}+m_{t,j}p^n)^2-Dd}{-4p^n}}{p}\right)\\ &= \left(\frac{\frac{(t_1p+tp^2+\cdot t_{n-2}p^{n-2}+tp^{n-1}+m_{t,j}p^n)^2-Dd}{-p^n}}{p}\right)\\ &= \left(\frac{\frac{(t_1p+t_2p^2+\cdots+t_{n-2}p^{n-2})^2-Dd}{-p^n} - 2t_1t}{p}\right).\end{aligned}$$

Since $p \nmid 2t_1$, we have $\sum_{t=0}^{p-1}\left(\frac{c_{t,j}}{p}\right) = 0$. Therefore,

$$N_{D,d}(p^n) = \frac{1}{2}\left(\frac{\pm\frac{d}{p}}{-p^n}\right)\sum_{i=1}^{4p}\left(\frac{c_i}{p}\right) = \frac{1}{2}\left(\frac{\pm\frac{d}{p}}{-p^n}\right)\sum_{t=1}^{p}2\sum_{j=1}^{2}\left(\frac{c_{t,j}}{p}\right) = \left(\frac{\pm\frac{d}{p}}{-p^n}\right)\sum_{j=1}^{2}\sum_{t=1}^{p}\left(\frac{c_{t,j}}{p}\right) = 0.$$

Thus, $N_{D,d}(p^n) = 0$ for $n \geq 4$. □

2.4.5 Case 1(iv)(b)

Proof of Proposition 2.8 in **Case 1(iv)(b)**. Recall the assumptions: $p \nmid f$, $p|d$ and $p|D_0$ with $p = 2$.

In this part of the sub-case, we will prove the same claims as the previous part:

I. $N_{D,d}(2) = 0$.

II. $N_{D,d}(2^2) = (-1)^{k+1}$.

III. $N_{D,d}(2^n) = 0$ for $n \geq 3$.

Then, we have

$$\begin{aligned}\sum_{n=0}^{\infty} \frac{(-1)^k N_{D,d}(2^n)}{2^{nk}} = 1 - \frac{1}{2^{2k}} &= 1 - 2^{-2k} \\ &= (1 + 2^{-k})(1 - 2^{-k}) \\ &= \frac{(1 + 2^{-k})(1 - 2^{-k})}{\left(1 - \left(\frac{D_0}{2}\right) \cdot 2^{-k}\right)\left(1 - \left(\frac{d}{2}\right) \cdot 2^{-k}\right)}\end{aligned}$$

since $\left(\frac{D_0}{2}\right) = \left(\frac{d}{2}\right) = 0$. □

Proof of Claim I. In this case, we know $d = 4m_1$ and $D_0 = 4m_2$ for $m_i \equiv 2$ or $3 \pmod 4$ and m_i squarefree. To determine $N_{D,d}(2)$, we look at the equation $b^2 - Dd \equiv 0 \pmod 8$. Since Dd is divisible by 16, the equation has two solutions, namely $b = 0$ or 4. Thus,

$$N_{D,d}(2) = \sum_{\substack{0 \leq b \leq 3 \\ b^2 \equiv Dd \pmod 8}} \chi_d\left(\left[-2, b, \frac{Dd - b^2}{8}\right]\right) = \chi_d\left(\left[-2, 0, \frac{Dd}{8}\right]\right). \tag{2.15}$$

Since $2|\frac{Dd}{8}$, $N_{D,d}(2) = \chi_d\left(\left[-2, 0, \frac{Dd}{8}\right]\right) = 0$. □

Proof of Claim II. Now, to determine $N_{D,d}(4)$, we look at the equation $b^2 - Dd \equiv 0 \pmod{16}$. Since $16|Dd$, we have $b^2 \equiv 0 \pmod{16}$ and the solutions are $0, 4, 8$ and 12. Let $c_0 = \frac{Dd}{16} = m_1 m_2 f^2$. Thus,

$$\begin{aligned}N_{D,d}(4) &= \chi_d\left(\left[-4, 0, \frac{Dd}{16}\right]\right) + \chi_d\left(\left[-4, 4, \frac{Dd - 16}{16}\right]\right) \\ &= \chi_d\left(\left[-4, 0, \frac{Dd}{16}\right]\right) + \chi_d\left(\left[-4, 4, \frac{Dd}{16} - 1\right]\right) \\ &= \chi_d\left([-4, 0, c_0]\right) + \chi_d\left([-4, 4, c_0 - 1]\right).\end{aligned}$$

First consider the case that $m_1 \equiv m_2 \equiv 3 \pmod 4$. Then, c_0-1 is even and $\chi_d([-4,4,c_0-1]) = 0$. Thus, we have

$$\begin{aligned}
N_{D,d}(4) &= \chi_d\left([-4,0,c_0]\right)\\
&= \left(\frac{-m_1}{-4}\right)\left(\frac{-4}{c_0}\right)\\
&= \left(\frac{-m_1}{-1}\right)\left(\frac{-1}{c_0}\right)\\
&= (-1)^{k+1}(-1)^{\frac{c_0-1}{2}}\\
&= (-1)^{k+1}.
\end{aligned}$$

because $c_0 \equiv 1 \pmod 4$.

Now, we consider the case that only one of the m_i is congruent to 2 modulo 4. In this case, c_0 is even and $\chi_d([-4,0,c_0]) = 0$. Thus, we have

$$\begin{aligned}
N_{D,d}(4) =&\chi_d([-4,4,c_0-1])\\
=&\begin{cases}
\left(\frac{-m_1}{-4}\right)\left(\frac{-4}{c_0-1}\right) & \text{if } m_1 \equiv 3 \pmod 4, m_2 \equiv 2 \pmod 4,\\
\left(\frac{\frac{m_1}{2}}{-4}\right)\left(\frac{8}{c_0-1}\right) & \text{if } m_1 \equiv 2 \pmod 8, m_2 \equiv 3 \pmod 4,\\
\left(\frac{-\frac{m_1}{2}}{-4}\right)\left(\frac{-8}{c_0-1}\right) & \text{if } m_1 \equiv 6 \pmod 8, m_2 \equiv 3 \pmod 4
\end{cases}\\
=&\begin{cases}
\left(\frac{-m_1}{-1}\right)\left(\frac{-1}{c_0-1}\right) & \text{if } m_1 \equiv 3 \pmod 4, m_2 \equiv 2 \pmod 4,\\
\left(\frac{\frac{m_1}{2}}{-1}\right)\left(\frac{2}{c_0-1}\right) & \text{if } m_1 \equiv 2 \pmod 8, m_2 \equiv 3 \pmod 4,\\
\left(\frac{-\frac{m_1}{2}}{-1}\right)\left(\frac{-2}{c_0-1}\right) & \text{if } m_1 \equiv 6 \pmod 8, m_2 \equiv 3 \pmod 4
\end{cases}\\
=&\begin{cases}
(-1)^{k+1}(-1)^{\frac{c_0-1-1}{2}} & \text{if } m_1 \equiv 3 \pmod 4, m_2 \equiv 2 \pmod 4,\\
(-1)^{k}\left(\frac{c_0-1}{2}\right) & \text{if } m_1 \equiv 2 \pmod 8, m_2 \equiv 3 \pmod 4,\\
(-1)^{k+1}\left(\frac{-1}{c_0-1}\right)\left(\frac{c_0-1}{2}\right) & \text{if } m_1 \equiv 6 \pmod 8, m_2 \equiv 3 \pmod 4
\end{cases}\\
=&\begin{cases}
(-1)^{k+1}(1) & \text{if } m_1 \equiv 3 \pmod 4, m_2 \equiv 2 \pmod 4,\\
(-1)^{k}(-1) & \text{if } m_1 \equiv 2 \pmod 8, m_2 \equiv 3 \pmod 4,\\
(-1)^{k+1}(1)(1) & \text{if } m_1 \equiv 6 \pmod 8, m_2 \equiv 3 \pmod 4
\end{cases}\\
=&(-1)^{k+1}.
\end{aligned}$$

Now we consider the case $m_1 \equiv m_2 \equiv 2 \pmod 4$. It is similar to the previous case and we have

$$\begin{aligned}
N_{D,d}(4) =& \chi_d([-4,4,c_0-1]) \\
=& \begin{cases} (-1)^k \left(\frac{c_0-1}{2}\right) & \text{if } m_1 \equiv 2 \pmod 8, m_2 \equiv 2 \pmod 4, \\ (-1)^{k+1} \left(\frac{-1}{c_0-1}\right)\left(\frac{c_0-1}{2}\right) & \text{if } m_1 \equiv 6 \pmod 8, m_2 \equiv 2 \pmod 4 \end{cases} \\
=& \begin{cases} (-1)^k(-1) & \text{if } m_1 \equiv 2 \pmod 8, m_2 \equiv 3 \pmod 4, \\ (-1)^{k+1}(-1)(-1) & \text{if } m_1 \equiv 6 \pmod 8, m_2 \equiv 3 \pmod 4 \end{cases} \\
=& (-1)^{k+1}.
\end{aligned}$$

□

Proof of Claim III. To find $N_{D,d}(8)$, we consider the equation $b^2 - Dd \equiv 0 \pmod{32}$. Recall that the equation $b^2 - Dd \equiv 0 \pmod{16}$ has the solution set $\{0, 4, 8, 12\}$.

If $m_1 \equiv m_2 \equiv 3 \pmod 4$, then 0 and 8 are not solutions to the equation $b^2 - Dd \equiv 0 \pmod{32}$ but 4 and 12 are. So they are lifted and now the equation $b^2 - Dd \equiv 0 \pmod{32}$ has the solution set $\{4, 12, 20, 28\}$. Let $c_0 = \frac{m_1 m_2 f^2 - 1}{2}$ Then, we have

$$\begin{aligned}
N_{D,d}(8) &= \chi_d\left(\left[-8, 4, \frac{Dd-16}{32}\right]\right) + \chi_d\left(\left[-8, 12, \frac{Dd-144}{32}\right]\right) \\
&= \chi_d\left(\left[-8, 4, \frac{16m_1m_2f^2-16}{32}\right]\right) + \chi_d\left(\left[-8, 12, \frac{16m_1m_2f^2-144}{32}\right]\right) \\
&= \chi_d\left(\left[-8, 4, \frac{m_1m_2f^2-1}{2}\right]\right) + \chi_d\left(\left[-8, 12, \frac{m_1m_2f^2-9}{2}\right]\right) \\
&= \chi_d\left([-8, 4, c_0]\right) + \chi_d\left([-8, 12, c_0-4]\right).
\end{aligned}$$

Note that c_0 and $c_0 - 4$ are both even because $m_1 m_2 f^2 \equiv 1 \pmod 4$. Thus $\chi_d([-8, 4, c_0]) = \chi_d([-8, 12, c_0 - 4]) = 0$ and $N_{D,d}(8) = 0$.

If at least one of the m_i is congruent to 2 modulo 4, then 0 and 8 are solutions to the equation $b^2 - Dd \equiv 0 \pmod{32}$ but not 4 and 12. Thus, 0 and 8 are lifted and the equation $b^2 - Dd \equiv 0 \pmod{32}$ has the solution set $\{0, 8, 16, 24\}$. Let $c_0 = \frac{m_1 m_2 f^2}{2}$. Thus,

$$\begin{aligned}
N_{D,d}(8) &= \chi_d\left(\left[-8, 0, \frac{16m_1m_2f^2}{32}\right]\right) + \chi_d\left(\left[-8, 8, \frac{16m_1m_2f^2-64}{32}\right]\right) \\
&= \chi_d([-8, 0, c_0]) + \chi_d([-8, 8, c_0-2]).
\end{aligned}$$

We first consider the case $m_1 \not\equiv m_2 \pmod 4$. Since c_0 is odd, both $\chi_d([-8,0,c_0]) \neq 0$ and $\chi_d([-8,8,c_0-2]) \neq 0$. Thus, we have

$$N_{D,d}(8) = \begin{cases} \left(\frac{-m_1}{-8}\right)\left(\frac{-4}{c_0}\right) + \left(\frac{-m_1}{-8}\right)\left(\frac{-4}{c_0-2}\right) & \text{if } m_1 \equiv 3 \pmod 4, m_2 \equiv 2 \pmod 4, \\ \left(\frac{\frac{m_1}{2}}{-8}\right)\left(\frac{8}{c_0}\right) + \left(\frac{\frac{m_1}{2}}{-8}\right)\left(\frac{8}{c_0-2}\right) & \text{if } m_1 \equiv 2 \pmod 8, m_2 \equiv 3 \pmod 4, \\ \left(\frac{-\frac{m_1}{2}}{-8}\right)\left(\frac{-8}{c_0}\right) + \left(\frac{-\frac{m_1}{2}}{-8}\right)\left(\frac{-8}{c_0-2}\right) & \text{if } m_1 \equiv 6 \pmod 8, m_2 \equiv 3 \pmod 4 \end{cases}$$

$$= \begin{cases} \left(\frac{-m_1}{-8}\right)\left[\left(\frac{-1}{c_0}\right) + \left(\frac{-1}{c_0-2}\right)\right] & \text{if } m_1 \equiv 3 \pmod 4, m_2 \equiv 2 \pmod 4, \\ \left(\frac{\frac{m_1}{2}}{-8}\right)\left[\left(\frac{2}{c_0}\right) + \left(\frac{2}{c_0-2}\right)\right] & \text{if } m_1 \equiv 2 \pmod 8, m_2 \equiv 3 \pmod 4, \\ \left(\frac{-\frac{m_1}{2}}{-8}\right)\left[\left(\frac{-2}{c_0}\right) + \left(\frac{-2}{c_0-2}\right)\right] & \text{if } m_1 \equiv 6 \pmod 8, m_2 \equiv 3 \pmod 4 \end{cases}$$

$$= \begin{cases} \left(\frac{-m_1}{-8}\right)\left[(-1)^{\frac{c_0-1}{2}} + (-1)^{\frac{c_0-2-1}{2}}\right] & \text{if } m_1 \equiv 3 \pmod 4, m_2 \equiv 2 \pmod 4, \\ \left(\frac{\frac{m_1}{2}}{-8}\right)\left[\left(\frac{c_0}{2}\right) + \left(\frac{c_0-2}{2}\right)\right] & \text{if } m_1 \equiv 2 \pmod 8, m_2 \equiv 3 \pmod 4, \\ \left(\frac{-\frac{m_1}{2}}{-8}\right)\left[\left(\frac{-1}{c_0}\right)\left(\frac{c_0}{2}\right) + \left(\frac{-1}{c_0-2}\right)\left(\frac{c_0-2}{2}\right)\right] & \text{if } m_1 \equiv 6 \pmod 8, m_2 \equiv 3 \pmod 4. \end{cases}$$

For the case $m_1 \equiv 3 \pmod 4, m_2 \equiv 2 \pmod 4$, we see that $(-1)^{\frac{c_0-1}{2}} + (-1)^{\frac{c_0-2-1}{2}} = 0$.

For the case $m_1 \equiv 2 \pmod 8, m_2 \equiv 3 \pmod 4$, we see that $\left(\frac{c_0}{2}\right) + \left(\frac{c_0-2}{2}\right) = 0$ because $c_0 \equiv 3 \pmod 4$.

For the case $m_1 \equiv 6 \pmod 8, m_2 \equiv 3 \pmod 4$, we see that

$$\left(\frac{-1}{c_0}\right)\left(\frac{c_0}{2}\right) + \left(\frac{-1}{c_0-2}\right)\left(\frac{c_0-2}{2}\right) = \left(\frac{-1}{c_0}\right)\left[\left(\frac{c_0}{2}\right) - \left(\frac{c_0-2}{2}\right)\right] = 0$$

because $c_0 \equiv 1 \pmod 4$.

Now we look at the case $m_1 \equiv m_2 \equiv 2 \pmod 4$. We have

$$N_{D,d}(8) = \chi_d([-8,0,c_0]) + \chi_d([-8,8,c_0-2]) = 0$$

because c_0 is even.

Now, we will prove $N_{D,d}(2^n) = 0$ for $n \geq 4$. We have seen that the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^2}$ has the solution set $\{0,4,8,12\} = \{0, 2^3, \pm 2^2\}$ and the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^3}$ has the solution set

$$\begin{cases} \{4,12,20,28\} = \{\pm 2^2, \pm(2^2+2^4)\} & \text{if } m_1 \equiv m_2 \equiv 3 \pmod 4 \text{ and,} \\ \{0,8,16,24\} = \{0, 2^4, \pm 2^3\} & \text{if } m_1 \equiv 2 \pmod 4 \text{ or } m_2 \equiv 2 \pmod 4. \end{cases} \tag{2.16}$$

We will first consider the case $m_1 \equiv m_2 \equiv 3 \pmod 4$. Rewrite the solution set $\{\pm 2^2, \pm(2^2 + 2^4)\} = \{\pm 2^2(2^2 m + 1)\}_{m=0}^{m=1}$ for the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^3}$. Then, for the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^4}$, we see that

$$\begin{aligned}[][2^2(2^2m+1)]^2 - 2^4 m_1 m_2 f^2 \equiv 0 \pmod{4 \cdot 2^4} &\iff (2^2m+1)^2 - m_1 m_2 f^2 \equiv 0 \pmod{2^2} \\ &\iff 1 - m_1 m_2 f^2 \equiv 0 \pmod{2^2},\end{aligned}$$

which is always true. Thus, the solution set $\{\pm 2^2(2^2 m + 1)\}_{m=0}^{m=1}$ is lifted. Then, the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^4}$ has the solution set

$$\begin{aligned}\{\pm 2^2(2^2m+1), \pm[2^2(2^2m+1) + 2^5\}_{m=0}^{m=1} &= \{\pm 2^2(2^2m+1), \pm 2^2[(2^2m+1) + 2^3]\}_{m=0}^{m=1} \\ &= \{\pm 2^2(2^2m+1), \pm 2^2[2^2(m+2)+1]\}_{m=0}^{m=1} \\ &= \{\pm 2^2(2^2m+1)\}_{m=0}^{m=3}.\end{aligned}$$

Note that in $N_{D,d}(2^n)$, it sums over the first half solutions $0 \leq b \leq 2 \cdot 2^n - 1$. If we write the solution set as $\{\pm b_i\}$, it is the same that we sum over the positive solutions. Let $c_m = \frac{Dd - (2^2(2^2m+1))^2}{4 \cdot 2^4} = \frac{m_1 m_2 f^2 - 1}{4} - 4m^2 - 2m = c_0 - 4m^2 - 2m$. Then,

$$\begin{aligned}N_{D,d}(2^4) &= \sum_{m=0}^{3} \chi_d([-2^4, 2^2(4m+1), c_m]) \\ &= \sum_{m=0}^{3} \left(\frac{-\frac{d}{4}}{-2^4}\right)\left(\frac{-4}{c_m}\right) \\ &= \begin{cases} \left(\frac{-\frac{d}{4}}{-2^4}\right) \sum_{m=0}^{3} \left(\frac{-1}{c_m}\right) & \text{if } c_0 \text{ is odd,} \\ 0 & \text{if } c_0 \text{ is even} \end{cases} \\ &= \begin{cases} \left(\frac{-\frac{d}{4}}{-2^4}\right) \left[(-1)^{\frac{c_0-1}{2}} + (-1)^{\frac{c_0-6-1}{2}} + (-1)^{\frac{c_0-20-1}{2}} + (-1)^{\frac{c_0-42-1}{2}}\right] & \text{if } c_0 \text{ is odd,} \\ 0 & \text{if } c_0 \text{ is even} \end{cases} \\ &= 0.\end{aligned}$$

For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^5}$, we see that

$$\begin{aligned}[][2^2(2^2m+1)]^2 - 2^4 m_1 m_2 f^2 \equiv 0 \pmod{4 \cdot 2^5} &\iff (2^2m+1)^2 - m_1 m_2 f^2 \equiv 0 \pmod{2^3} \\ &\iff 1 - m_1 m_2 f^2 \equiv 0 \pmod{2^3},\end{aligned}$$

which is true only if $m_1 m_2 f^2 \equiv 1 \pmod{2^3}$. If $m_1 m_2 f^2 \equiv 5 \pmod{2^3}$, $1 - m_1 m_2 f^2 \equiv 0 \pmod{2^3}$ is not true. Thus, the solution set $\{\pm 2^2(2^2m+1)\}_{m=0}^{m=3}$ is lifted only if $m_1 m_2 f^2 \equiv 1 \pmod{2^3}$, otherwise there is no solution. Thus, if $m_1m_2f^2 \equiv 1 \pmod{2^3}$, the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^5}$ has the solution set

$$\begin{aligned}\{\pm 2^2(2^2m+1), \pm[2^2(2^2m+1)+2^6\}_{m=0}^{m=3} &= \{\pm 2^2(2^2m+1), \pm 2^2[(2^2m+1)+2^4]\}_{m=0}^{m=3} \\ &= \{\pm 2^2(2^2m+1), \pm 2^2[2^2(m+2^2)+1]\}_{m=0}^{m=3} \\ &= \{\pm 2^2(2^2m+1)\}_{m=0}^{m=7}.\end{aligned}$$

So, if $m_1m_2f^2 \equiv 5 \pmod{2^3}$, $N_{D,d}(2^5) = 0$ and $N_{D,d}(2^n) = 0$ for $n \geq 5$. Assume $m_1m_2f^2 \equiv 1 \pmod{2^3}$. Let $c_m = \frac{Dd-(2^2(2^2m+1))^2}{4 \cdot 2^5} = \frac{m_1m_2f^2-1}{8} - 2m^2 - m = c_0 - 2m^2 - m$. Then,

$$\begin{aligned}N_{D,d}(2^5) &= \sum_{m=0}^{7} \chi_d([-2^4, 2^2(2^2m+1), c_m]) \\ &= \sum_{m=0}^{7} \left(\frac{-\frac{d}{4}}{-2^5}\right)\left(\frac{-4}{c_m}\right) \\ &= \begin{cases} \left(\frac{-\frac{d}{4}}{-2^5}\right)\left[\left(\frac{-1}{c_0}\right)+\left(\frac{-1}{c_2}\right)+\left(\frac{-1}{c_4}\right)+\left(\frac{-1}{c_6}\right)\right] & \text{if } c_0 \text{ is odd,} \\ \left(\frac{-\frac{d}{4}}{-2^5}\right)\left[\left(\frac{-1}{c_1}\right)+\left(\frac{-1}{c_3}\right)+\left(\frac{-1}{c_5}\right)+\left(\frac{-1}{c_7}\right)\right] & \text{if } c_0 \text{ is even} \end{cases} \\ &= \begin{cases} \left(\frac{-\frac{d}{4}}{-2^5}\right)\left[(-1)^{\frac{c_0-1}{2}}+(-1)^{\frac{c_0-10-1}{2}}+(-1)^{\frac{c_0-36-1}{2}}+(-1)^{\frac{c_0-78-1}{2}}\right] & \text{if } c_0 \text{ is odd,} \\ \left(\frac{-\frac{d}{4}}{-2^5}\right)\left[(-1)^{\frac{c_0-3-1}{2}}+(-1)^{\frac{c_0-21-1}{2}}+(-1)^{\frac{c_0-55-1}{2}}+(-1)^{\frac{c_0-105-1}{2}}\right] & \text{if } c_0 \text{ is even} \end{cases} \\ &= 0.\end{aligned}$$

For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^6}$, we see that

$$\begin{aligned}[2^2(2^2m+1)]^2 - 2^4m_1m_2f^2 \equiv 0 \pmod{4 \cdot 2^6} &\iff (2^2m+1)^2 - m_1m_2f^2 \equiv 0 \pmod{2^4} \\ &\iff 2^3m + 1 - m_1m_2f^2 \equiv 0 \pmod{2^4}.\end{aligned}$$

If $m_1m_2f^2 \equiv 1 \pmod{2^4}$,

$$\begin{aligned}2^3m + 1 - m_1m_2f^2 \equiv 0 \pmod{2^4} &\iff 2^3m \equiv 0 \pmod{2^4} \\ &\iff m \text{ is even.}\end{aligned}$$

Thus, the solution set will be

$$\begin{aligned}\{\pm 2^2(2^2m+1), \pm[2^2(2^2m+1)+2^7]\}_{m=0,2,4,6} &= \{\pm 2^2(2^3m+1), \pm[2^2(2^3m+1)+2^7]\}_{m=0}^{m=3}\\ &= \{\pm 2^2(2^3m+1), \pm 2^2[(2^3m+1)+2^5]\}_{m=0}^{m=3}\\ &= \{\pm 2^2(2^2m+1), \pm 2^2[2^3(m+2^2)+1]\}_{m=0}^{m=3}\\ &= \{\pm 2^2(2^3m+1)\}_{m=0}^{m=7}.\end{aligned}$$

If $m_1m_2f^2 \equiv 2^3+1 \pmod{2^4}$,

$$\begin{aligned}2^3m+1-m_1m_2f^2 \equiv 0 \pmod{2^4} &\Longleftrightarrow 2^3m-2^3 \equiv 0 \pmod{2^4}\\ &\Longleftrightarrow 2^3(m-1) \equiv 0 \pmod{2^4}\\ &\Longleftrightarrow m-1 \equiv 0 \pmod{2}\\ &\Longleftrightarrow m \text{ is odd.}\end{aligned}$$

Thus, the solution set will be

$$\begin{aligned}\{\pm 2^2(2^2m+1), \pm[2^2(2^2m+1)+2^7]\}_{m=1,3,5,7} &= \{\pm 2^2(2^2(2m+1)+1), \pm[2^2(2^2(2m+1)+1)+2^7]\}_{m=0}^{m=3}\\ &= \{\pm 2^2(2^3m+2^2+1), \pm 2^2[2^3m+2^2+1+2^5]\}_{m=0}^{m=3}\\ &= \{\pm 2^2(2^3m+2^2+1), \pm 2^2[2^3(m+2^2)+2^2+1]\}_{m=0}^{m=3}\\ &= \{\pm 2^2(2^3m+2^2+1)\}_{m=0}^{m=7}.\end{aligned}$$

From now on, the pattern is similar. For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^n}$ with $n \geq 6$, if $m_1m_2f^2 \equiv 2^3r+1 \pmod{2^{n-2}}$ for some $r \in \{0, 1, ..., 2^{n-5}-1\}$, it has the solution set of the form $\{\pm 2^2(2^{n-3}m+2^2t+1)\}_{m=0}^{m=7}$ for some $t \in \{0, 1, ..., 2^{n-5}-1\}$ with $(2^2t+1)^2 \equiv 2^3r+1 \pmod{2^{n-2}}$. We will show this by induction.

We have shown the first case is true when $n=6$. Now for the equation $b^2-Dd \equiv 0 \pmod{4 \cdot 2^{n+1}}$, we see that

$$\begin{aligned}[2^2(2^{n-3}m+2^2t+1)]^2 - 2^4m_1m_2f^2 \equiv 0 \pmod{4 \cdot 2^{n+1}} &\Longleftrightarrow (2^{n-3}m+2^2t+1)^2 - m_1m_2f^2 \equiv 0 \pmod{2^{n-1}}\\ &\Longleftrightarrow 2^{n-2}m+(2^2t+1)^2-m_1m_2f^2 \equiv 0 \pmod{2^{n-1}}.\end{aligned}$$

If $m_1m_2f^2 \equiv 2^3r+1 \pmod{2^{n-1}}$ and $(2^2t+1)^2 \equiv 2^3r+1 \pmod{2^{n-1}}$, then

$$\begin{aligned}2^{n-2}m+(2^2t+1)^2-m_1m_2f^2 \equiv 0 \pmod{2^{n-1}} &\Longleftrightarrow 2^{n-2}m \equiv 0 \pmod{2^{n-1}}\\ &\Longleftrightarrow m \text{ is even.}\end{aligned}$$

If $m_1m_2f^2 \equiv 2^{n-2} + 2^3r + 1 \pmod{2^{n-1}}$ and $(2^2t+1)^2 \equiv 2^{n-2} + 2^3r + 1 \pmod{2^{n-1}}$, then

$$\begin{aligned} 2^{n-2}m + (2^2t+1)^2 - m_1m_2f^2 \equiv 0 \pmod{2^{n-1}} \iff & 2^{n-2}m \equiv 0 \pmod{2^{n-1}} \\ \iff & m \text{ is even.} \end{aligned}$$

In either case, the solution set will be

$$\begin{aligned} &\{\pm 2^2(2^{n-3}m + 2^2t + 1), \pm[2^2(2^{n-3}m + 2^2t + 1) + 2^{n+2}]\}_{m=0,2,4,6} \\ =&\{\pm 2^2(2^{n-2}m + 2^2t + 1), \pm[2^2(2^{n-2}m + 2^2t + 1) + 2^{n+2}]\}_{m=0}^{m=3} \\ =&\{\pm 2^2(2^{n-2}m + 2^2t + 1), \pm 2^2[(2^{n-2}m + 2^2t + 1) + 2^{n}]\}_{m=0}^{m=3} \\ =&\{\pm 2^2(2^{n-2}m + 2^2t + 1), \pm 2^2[2^{n-2}(m + 2^2) + 2^2t + 1]\}_{m=0}^{m=3} \\ =&\{\pm 2^2(2^{n-2}m + 2^2t + 1)\}_{m=0}^{m=7}. \end{aligned}$$

If $m_1m_2f^2 \equiv 2^{n-2} + 2^3r + 1 \pmod{2^{n-1}}$ and $(2^2t+1)^2 \equiv 2^3r + 1 \pmod{2^{n-1}}$, then

$$\begin{aligned} 2^{n-2}m + (2^2t+1)^2 - m_1m_2f^2 \equiv 0 \pmod{2^{n-1}} \iff & 2^{n-2}m - 2^{n-2} \equiv 0 \pmod{2^{n-1}} \\ \iff & m \text{ is odd.} \end{aligned}$$

If $m_1m_2f^2 \equiv 2^3r + 1 \pmod{2^{n-1}}$ and $(2^2t+1)^2 \equiv 2^{n-2} + 2^3r + 1 \pmod{2^{n-1}}$, then

$$\begin{aligned} 2^{n-2}m + (2^2t+1)^2 - m_1m_2f^2 \equiv 0 \pmod{2^{n-1}} \iff & 2^{n-2}m + 2^{n-2} \equiv 0 \pmod{2^{n-1}} \\ \iff & m \text{ is odd.} \end{aligned}$$

Either case, the solution set will be

$$\begin{aligned} &\{\pm 2^2(2^{n-3}m + 2^2t + 1), \pm[2^2(2^{n-3}m + 2^2t + 1) + 2^{n+2}]\}_{m=1,3,5,7} \\ =&\{\pm 2^2(2^{n-3}(2m+1) + 2^2t + 1), \pm[2^2(2^{n-3}(2m+1) + 2^2t + 1) + 2^{n+2}]\}_{m=1,3,5,7} \\ =&\{\pm 2^2(2^{n-2}m + 2^{n-3} + 2^2t + 1), \pm[2^2(2^{n-2}m + 2^{n-3} + 2^2t + 1) + 2^{n+2}]\}_{m=0}^{m=3} \\ =&\{\pm 2^2(2^{n-2}m + 2^{n-3} + 2^2t + 1), \pm 2^2[(2^{n-2}m + 2^{n-3} + 2^2t + 1) + 2^{n}]\}_{m=0}^{m=3} \\ =&\{\pm 2^2(2^{n-2}m + 2^{n-3} + 2^2t + 1), \pm 2^2[2^{n-2}(m + 2^2) + 2^{n-3} + 2^2t + 1]\}_{m=0}^{m=3} \\ =&\{\pm 2^2(2^{n-2}m + 2^{n-3} + 2^2t + 1)\}_{m=0}^{m=7} \\ =&\{\pm 2^2(2^{n-2}m + 2^2(2^{n-5} + t) + 1)\}_{m=0}^{m=7}. \end{aligned}$$

Thus, the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{n+1}}$, if $m_1m_2f^2 \equiv 2^3r + 1 \pmod{2^{n-1}}$ for some $r \in \{0, 1, ..., 2^{n-4} - 1\}$, it has the solution set of the form $\{\pm 2^2(2^{n-2}m + 2^2t + 1)\}_{m=0}^{m=7}$ for some $t \in \{0, 1, ..., 2^{n-4} - 1\}$ with $(2^2t+1)^2 \equiv 2^3r + 1 \pmod{2^{n-1}}$. The induction is done.

Let $c_m = \dfrac{Dd - [2^2(2^{n-3}m + 2^2t + 1)]^2}{4 \cdot 2^n} = \dfrac{m_1 m_2 f^2 - (2^{n-3}m + 2^2t + 1)^2}{2^{n-2}} = \dfrac{m_1 m_2 f^2 - 1 - 8t - 16t^2}{2^{n-2}} - 2^{n-4}m^2 - 4tm - m = c_0 - 2^{n-4}m^2 - 4tm - m.$

$$
\begin{aligned}
N_{D,d}(2^n) &= \sum_{m=0}^{7} \chi_d([-2^n, 2^2(1 + 4t + 2^{n-3}m), c_m]) \\
&= \sum_{m=0}^{7} \left(\frac{-\frac{d}{4}}{-2^n}\right)\left(\frac{-4}{c_m}\right) \\
&= \begin{cases} \left(\frac{-\frac{d}{4}}{-2^n}\right)\left[\left(\frac{-1}{c_0}\right) + \left(\frac{-1}{c_2}\right) + \left(\frac{-1}{c_4}\right) + \left(\frac{-1}{c_6}\right)\right] & \text{if } c_0 \text{ is odd,} \\ \left(\frac{-\frac{d}{4}}{-2^n}\right)\left[\left(\frac{-1}{c_1}\right) + \left(\frac{-1}{c_3}\right) + \left(\frac{-1}{c_5}\right) + \left(\frac{-1}{c_7}\right)\right] & \text{if } c_0 \text{ is even} \end{cases} \\
&= \begin{cases} \left(\frac{-\frac{d}{4}}{-2^n}\right)\left[(-1)^{\frac{c_0-1}{2}} + (-1)^{\frac{c_0-2^{n-2}-8t-2-1}{2}}\right. & \text{if } c_0 \text{ is odd,} \\ \left. +(-1)^{\frac{c_0-2^n-16t-4-1}{2}} + (-1)^{\frac{c_0-2^{n-2}3^2-24t-6-1}{2}}\right] & \\ \left(\frac{-\frac{d}{4}}{-2^n}\right)\left[(-1)^{\frac{c_0-2^{n-4}-4t-1-1}{2}} + (-1)^{\frac{c_0-2^{n-4}3^2-12t-3-1}{2}}\right. & \text{if } c_0 \text{ is even} \\ \left. +(-1)^{\frac{c_0-2^{n-4}5^2-20t-5-1}{2}} + (-1)^{\frac{c_0-2^{n-4}7^2-28t-7-1}{2}}\right] & \end{cases} \\
&= 0.
\end{aligned}
$$

Thus, $N_{D,d}(2^n) = 0$ for $n \geq 6$. □

Now, assume $m_1 \equiv m_2 \equiv 2 \pmod 4$. The process is similar. Remember the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^3}$ has the solution set $\{0, 2^4, \pm 2^3\} = \{2^3 m\}_{m=0}^{m=3}$. We check that each solution is lifted and thus the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^4}$ has the solution set $\{0, 2^5, \pm 2^4, \pm 2^3, \pm(2^3 + 2^5)\} = \{\pm 2^3 m\}_{m=0}^{m=3}$. Now, we have

$$
\begin{aligned}
N_{D,d}(2^4) &= \sum_{m=0}^{3} \chi_d([-2^4, 2^3 m, c_m]) \quad \text{where } c_m = \frac{Dd - (2^3m)^2}{4 \cdot 2^4} = \frac{m_1}{2}\frac{m_2}{2}f^2 - m^2 = c_0 - m^2, \\
&= \begin{cases} \sum_{m=0}^{3} \left(\frac{\frac{d}{8}}{-2^4}\right)\left(\frac{8}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4, \\ \sum_{m=0}^{3} \left(\frac{\frac{d}{-8}}{-2^4}\right)\left(\frac{-8}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4 \end{cases} \\
&= \begin{cases} \left(\frac{\frac{d}{8}}{-2^4}\right)\sum_{m=0}^{3} \left(\frac{2}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4, \\ \left(\frac{\frac{d}{-8}}{-2^4}\right)\sum_{m=0}^{3} \left(\frac{-2}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4. \end{cases}
\end{aligned}
$$

Consider that

$$\begin{aligned}\sum_{m=0}^{3}\left(\frac{2}{c_m}\right) &= \sum_{m=0}^{3}\left(\frac{c_m}{2}\right)\\ &= \left(\frac{c_0}{2}\right)+\left(\frac{c_0-1}{2}\right)+\left(\frac{c_0-4}{2}\right)+\left(\frac{c_0-9}{2}\right)\\ &= \left(\frac{c_0}{2}\right)+\left(\frac{c_0-4}{2}\right) \qquad \text{since } c_0=\frac{m_1}{2}\frac{m_2}{2}f^2 \text{ is odd.}\\ &= 0.\end{aligned}$$

Also consider

$$\begin{aligned}&\sum_{m=0}^{3}\left(\frac{-2}{c_m}\right)\\ =&\sum_{m=0}^{3}\left(\frac{-1}{c_m}\right)\left(\frac{2}{c_m}\right)\\ =&\sum_{m=0}^{3}\left(\frac{-1}{c_m}\right)\left(\frac{c_m}{2}\right)\\ =&\left(\frac{-1}{c_0}\right)\left(\frac{c_0}{2}\right)+\left(\frac{-1}{c_0-1}\right)\left(\frac{c_0-1}{2}\right)+\left(\frac{-1}{c_0-4}\right)\left(\frac{c_0-4}{2}\right)+\left(\frac{-1}{c_0-9}\right)\left(\frac{c_0-9}{2}\right)\\ =&\left(\frac{-1}{c_0}\right)\left(\frac{c_0}{2}\right)+\left(\frac{-1}{c_0-4}\right)\left(\frac{c_0-4}{2}\right)\\ =&(-1)^{\frac{c_0-1}{2}}\left(\frac{c_0}{2}\right)+(-1)^{\frac{c_0-4-1}{2}}\left(\frac{c_0-4}{2}\right)\\ =&(-1)^{\frac{c_0-1}{2}}\left[\left(\frac{c_0}{2}\right)+\left(\frac{c_0-4}{2}\right)\right]\\ =&0.\end{aligned}$$

Thus, $N_{D,d}(2^4)=0$.

For the equation $b^2-Dd\equiv 0 \pmod{4\cdot 2^5}$, the solutions $0,\pm 2^4$ and 2^5 from before are not lifted but the others are, so we have the solution set $\{\pm 2^3, \pm(2^3+2^5), \pm(2^3+2^6), \pm(2^3+2^5+2^6)\} = \{\pm 2^3(2^2m+1)\}_{m=0}^{m=3}$. Let $c_m = \dfrac{Dd-[2^3(2^2m+1)]^2}{4\cdot 2^5} = \dfrac{\frac{m_1}{2}\frac{m_2}{2}f^2-(4m+1)^2}{2} = \dfrac{\frac{m_1}{2}\frac{m_2}{2}f^2-1}{2} - 8m^2-4m = c_0-8m^2-4m$. Then,

$$N_{D,d}(2^5) = \sum_{m=0}^{3} \chi_d([-2^5, 2^3(4m+1), c_m])$$
$$= \begin{cases} \sum_{m=0}^{3} \left(\frac{\frac{d}{8}}{-2^5}\right)\left(\frac{8}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4, \\ \sum_{m=0}^{3} \left(\frac{\frac{d}{-8}}{-2^5}\right)\left(\frac{-8}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4 \end{cases}$$
$$= \begin{cases} \left(\frac{\frac{d}{8}}{-2^5}\right)\sum_{m=0}^{3} \left(\frac{2}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4, \\ \left(\frac{\frac{d}{-8}}{-2^5}\right)\sum_{m=0}^{3} \left(\frac{-2}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4. \end{cases}$$

Consider that

$$\begin{aligned} \sum_{m=0}^{3} \left(\frac{2}{c_m}\right) &= \sum_{m=0}^{3} \left(\frac{c_m}{2}\right) \\ &= \left(\frac{c_0}{2}\right) + \left(\frac{c_0-12}{2}\right) + \left(\frac{c_0-16}{2}\right) + \left(\frac{c_0-60}{2}\right) \\ &= 2\left[\left(\frac{c_0}{2}\right) + \left(\frac{c_0-4}{2}\right)\right] \\ &= 0. \end{aligned}$$

Also consider

$$\begin{aligned} &\sum_{m=0}^{3} \left(\frac{-2}{c_m}\right) \\ =&\sum_{m=0}^{3} \left(\frac{-1}{c_m}\right)\left(\frac{2}{c_m}\right) \\ =&\sum_{m=0}^{3} \left(\frac{-1}{c_m}\right)\left(\frac{c_m}{2}\right) \\ =&(-1)^{\frac{c_0-1}{2}}\left(\frac{c_0}{2}\right) + (-1)^{\frac{c_0-12-1}{2}}\left(\frac{c_0-12}{2}\right) + (-1)^{\frac{c_0-16-1}{2}}\left(\frac{c_0-16}{2}\right) + (-1)^{\frac{c_0-60-1}{2}}\left(\frac{c_0-60}{2}\right) \\ =&2(-1)^{\frac{c_0-1}{2}}\left[\left(\frac{c_0}{2}\right) + \left(\frac{c_0-4}{2}\right)\right] \\ =&0. \end{aligned}$$

Thus, $N_{D,d}(2^5) = 0$.

For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^6}$, all solutions from before are lifted only if $\frac{m_1}{2}\frac{m_2}{2}f^2 \equiv 1 \pmod{2^2}$ and otherwise the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^6}$ has no solution and $N_{D,d}(2^n) = 0$ for $n \geq 6$. Thus, assume $\frac{m_1}{2}\frac{m_2}{2}f^2 \equiv 1 \pmod{2^2}$. Then the solution set will be $\{\pm 2^3(2^2m+1)\}_{m=0}^{m=7}$. Let $c_m = \frac{Dd-(2^3(2^2m+1))^2}{4 \cdot 2^6} = \frac{\frac{m_1}{2}\frac{m_2}{2}f^2-(2^2m+1)^2}{4} = \frac{\frac{m_1}{2}\frac{m_2}{2}f^2-1}{4} - 4m^2 - 2m = c_0 - 4m^2 - 2m$. Then,

$$N_{D,d}(2^6) = \sum_{m=0}^{7} \chi_d([-2^6, 2^3(2m+1), c_m]) = \begin{cases} \sum_{m=0}^{7} \left(\frac{\frac{d}{8}}{-2^6}\right)\left(\frac{8}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4, \\ \sum_{m=0}^{7} \left(\frac{\frac{d}{-8}}{-2^6}\right)\left(\frac{-8}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4 \end{cases}$$

$$= \begin{cases} \left(\frac{\frac{d}{8}}{-2^6}\right) \sum_{m=0}^{7} \left(\frac{2}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4, \\ \left(\frac{\frac{d}{-8}}{-2^6}\right) \sum_{m=0}^{7} \left(\frac{-2}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4. \end{cases}$$

Consider that

$$\begin{aligned}\sum_{m=0}^{7}\left(\frac{2}{c_m}\right) = \sum_{m=0}^{7}\left(\frac{c_m}{2}\right) = &\left(\frac{c_0}{2}\right) + \left(\frac{c_0-6}{2}\right) + \left(\frac{c_0-20}{2}\right) + \left(\frac{c_0-42}{2}\right) + \\ &\left(\frac{c_0-72}{2}\right) + \left(\frac{c_0-110}{2}\right) + \left(\frac{c_0-156}{2}\right) + \left(\frac{c_0-210}{2}\right) \\ =&2\left[\left(\frac{c_0}{2}\right) + \left(\frac{c_0-2}{2}\right) + \left(\frac{c_0-4}{2}\right) + \left(\frac{c_0-6}{2}\right)\right] \\ =&0.\end{aligned}$$

Also consider

$$\begin{aligned}&\sum_{m=0}^{7}\left(\frac{-2}{c_m}\right) = \sum_{m=0}^{7}\left(\frac{-1}{c_m}\right)\left(\frac{2}{c_m}\right) = \sum_{m=0}^{7}\left(\frac{-1}{c_m}\right)\left(\frac{c_m}{2}\right) \\ =&(-1)^{\frac{c_0-1}{2}}\left(\frac{c_0}{2}\right) + (-1)^{\frac{(c_0-2)-1}{2}}\left(\frac{c_0-2}{2}\right) + (-1)^{\frac{(c_0-6)-1}{2}}\left(\frac{c_0-6}{2}\right) + (-1)^{\frac{(c_0-12)-1}{2}}\left(\frac{c_0-12}{2}\right) \\ &(-1)^{\frac{(c_0-20)-1}{2}}\left(\frac{c_0-20}{2}\right) + (-1)^{\frac{(c_0-30)-1}{2}}\left(\frac{c_0-30}{2}\right) + (-1)^{\frac{(c_0-42)-1}{2}}\left(\frac{c_0-42}{2}\right) \\ &+ (-1)^{\frac{(c_0-56)-1}{2}}\left(\frac{c_0-56}{2}\right) \qquad \text{(we can assume } c_0 \text{ is odd.)} \\ =&(-1)^{\frac{c_0-1}{2}}\left(\frac{c_0}{2}\right) + (-1)^{\frac{c_0-1}{2}-1}\left(\frac{c_0-2}{2}\right) + (-1)^{\frac{c_0-1}{2}-1}\left(\frac{c_0-6}{2}\right) + (-1)^{\frac{c_0-1}{2}}\left(\frac{c_0-4}{2}\right) \\ &(-1)^{\frac{c_0-1}{2}}\left(\frac{c_0-4}{2}\right) + (-1)^{\frac{c_0-1}{2}-1}\left(\frac{c_0-6}{2}\right) + (-1)^{\frac{c_0-1}{2}-1}\left(\frac{c_0-2}{2}\right) + (-1)^{\frac{c_0-1}{2}}\left(\frac{c_0}{2}\right) \\ =&2(-1)^{\frac{c_0-1}{2}}\left[\left(\frac{c_0}{2}\right) - \left(\frac{c_0-2}{2}\right) - \left(\frac{c_0-6}{2}\right) + \left(\frac{c_0-4}{2}\right)\right] \\ =&0.\end{aligned}$$

Thus, $N_{D,d}(2^6) = 0$.

For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^7}$, all solutions from before are lifted if $m_1 m_2 f^2 \equiv 4 \pmod{2^5}$ and otherwise no solution. Thus, assume $m_1 m_2 f^2 \equiv 4 \pmod{2^5}$. Then the solution set will be $\{\pm 2^3(2^2 m+1)\}_{m=0}^{m=15}$. Let $c_m = \frac{Dd-(2^3(2^2m+1))^2}{4\cdot 2^7} = \frac{\frac{m_1}{2}\frac{m_2}{2}f^2-(4m+1)^2}{8} = \frac{\frac{m_1}{2}\frac{m_2}{2}f^2-1}{8} - 2m^2 - m = c_0 - 2m^2 - m$.

$$N_{D,d}(2^7) = \sum_{m=0}^{15} \chi_d([-2^7, 2^3(2^2m+1), c_m]) = \begin{cases} \sum_{m=0}^{15} \left(\frac{\frac{d}{8}}{-2^7}\right)\left(\frac{8}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4, \\ \sum_{m=0}^{15} \left(\frac{\frac{d}{-8}}{-2^7}\right)\left(\frac{-8}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4 \end{cases}$$

$$= \begin{cases} \left(\frac{\frac{d}{8}}{-2^7}\right) \sum_{m=0}^{15} \left(\frac{2}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4, \\ \left(\frac{\frac{d}{-8}}{-2^7}\right) \sum_{m=0}^{15} \left(\frac{-2}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4. \end{cases}$$

Consider that

$$\begin{aligned}
&\sum_{m=0}^{15} \left(\frac{2}{c_m}\right) \\
=&\sum_{m=0}^{15} \left(\frac{c_m}{2}\right) \\
=&\left(\frac{c_0}{2}\right) + \left(\frac{c_0-3}{2}\right) + \left(\frac{c_0-10}{2}\right) + \left(\frac{c_0-21}{2}\right) + \left(\frac{c_0-36}{2}\right) + \left(\frac{c_0-55}{2}\right) + \left(\frac{c_0-78}{2}\right) \\
&+ \left(\frac{c_0-105}{2}\right) + \left(\frac{c_0-136}{2}\right) + \left(\frac{c_0-171}{2}\right) + \left(\frac{c_0-210}{2}\right) + \left(\frac{c_0-253}{2}\right) + \left(\frac{c_0-300}{2}\right) \\
&\left(\frac{c_0-351}{2}\right) + \left(\frac{c_0-406}{2}\right) + \left(\frac{c_0-465}{2}\right) \\
=&\left(\frac{c_0}{2}\right) + \left(\frac{c_0-3}{2}\right) + \left(\frac{c_0-2}{2}\right) + \left(\frac{c_0-5}{2}\right) + \left(\frac{c_0-4}{2}\right) + \left(\frac{c_0-7}{2}\right) + \left(\frac{c_0-6}{2}\right) \\
&+ \left(\frac{c_0-1}{2}\right) + \left(\frac{c_0}{2}\right) + \left(\frac{c_0-3}{2}\right) + \left(\frac{c_0-2}{2}\right) + \left(\frac{c_0-5}{2}\right) + \left(\frac{c_0-4}{2}\right) \\
&\left(\frac{c_0-7}{2}\right) + \left(\frac{c_0-6}{2}\right) + \left(\frac{c_0-1}{2}\right) \\
=&0.
\end{aligned}$$

Also consider

$$\begin{aligned}\sum_{m=0}^{15}\left(\frac{-2}{c_m}\right) &= \sum_{m=0}^{15}\left(\frac{-1}{c_m}\right)\left(\frac{2}{c_m}\right)\\ &= \sum_{m=0}^{15}\left(\frac{-1}{c_m}\right)\left(\frac{c_m}{2}\right)\\ &= \begin{cases} 2(-1)^{\frac{c_0-1}{2}}\left[\left(\frac{c_0}{2}\right)-\left(\frac{c_0-6}{2}\right)-\left(\frac{c_0-2}{2}\right)+\left(\frac{c_0-4}{2}\right)\right] & \text{if } c_0 \text{ is odd,}\\ 2(-1)^{\frac{c_0-2}{2}}\left[\left(\frac{c_0-1}{2}\right)-\left(\frac{c_0-3}{2}\right)-\left(\frac{c_0-7}{2}\right)+\left(\frac{c_0-5}{2}\right)\right] & \text{if } c_0 \text{ is even}\end{cases}\\ &=0.\end{aligned}$$

Thus, $N_{D,d}(2^7) = 0$.

For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^8}$, if $\frac{m_1}{2}\frac{m_2}{2}f^2 \equiv 1 \pmod{2^6}$, the solution set is $\{\pm 2^3(2^3m+1)\}_{m=0}^{m=15}$. If $\frac{m_1}{2}\frac{m_2}{2}f^2 \equiv 2^3+1 \pmod{2^4}$, the solution set is $\{\pm 2^3(2^3m+2^2+1)\}_{m=0}^{m=15}$.

From now on, the pattern is similar. By the same induction argument, for the equation $b^2-Dd \equiv 0 \pmod{4\cdot 2^n}$ with $n \geq 8$, if $\frac{m_1}{2}\frac{m_2}{2}f^2 \equiv 2^3r+1 \pmod{2^{n-4}}$ for some $r \in \{0,1,...,2^{n-7}-1\}$, the solution set is of the form $\{\pm 2^3(2^{n-5}m+2^2t+1)\}_{m=0}^{m=15}$ for some $t \in \{0,1,...,2^{n-7}-1\}$ with $(2^2t+1)^2 \equiv 2^3r+1 \pmod{2^{n-2}}$.

Let $c_m = \frac{Dd-[2^3(2^{n-5}m+2^2t+1)]^2}{4\cdot 2^n} = \frac{\frac{m_1}{2}\frac{m_2}{2}f^2-(2^{n-5}m+4t+1)^2}{2^{n-4}} = \frac{\frac{m_1}{2}\frac{m_2}{2}f^2-1-8t-16t^2}{2^{n-4}} - 2^{n-6}m^2-4tm-m = c_0 - 2^{n-6}m^2 - 4tm - m$.

$$\begin{aligned}N_{D,d}(2^n) &= \sum_{m=0}^{15}\chi_d([-2^n, 2^3(1+4t+2^{n-5}m), c_m])\\ &= \begin{cases}\sum_{m=0}^{15}\left(\frac{\frac{d}{8}}{-2^n}\right)\left(\frac{8}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4,\\ \sum_{m=0}^{15}\left(\frac{\frac{d}{-8}}{-2^n}\right)\left(\frac{-8}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4\end{cases}\\ &= \begin{cases}\left(\frac{\frac{d}{8}}{-2^n}\right)\sum_{m=0}^{15}\left(\frac{2}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4,\\ \left(\frac{\frac{d}{-8}}{-2^n}\right)\sum_{m=0}^{15}\left(\frac{-2}{c_m}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4\end{cases}\end{aligned}$$

Consider that

$$\begin{aligned}
&\sum_{m=0}^{15}\left(\frac{2}{c_m}\right)\\
=&\sum_{m=0}^{15}\left(\frac{c_m}{2}\right)\\
=&\begin{cases}\sum_{m=0}^{7}\left(\frac{c_{2m}}{2}\right) & \text{if } c_0 \text{ is odd,}\\ \sum_{m=0}^{7}\left(\frac{c_{2m+1}}{2}\right) & \text{if } c_0 \text{ is even}\end{cases}\\
=&\begin{cases}2\left[\left(\frac{c_0}{2}\right)+\left(\frac{c_0-2}{2}\right)+\left(\frac{c_0-4}{2}\right)+\left(\frac{c_0-6}{2}\right)\right] & \text{if } c_0 \text{ is odd,}\\ 2\left[\left(\frac{c_0-2^{n-6}-4t-1}{2}\right)+\left(\frac{c_0-2^{n-6}-4t-3}{2}\right)+\left(\frac{c_0-2^{n-6}-4t-5}{2}\right)+\left(\frac{c_0-2^{n-6}-4t-7}{2}\right)\right] & \text{if } c_0 \text{ is even}\end{cases}\\
=&0.
\end{aligned}$$

Also consider

$$\begin{aligned}
\sum_{m=0}^{15}\left(\frac{-2}{c_m}\right)=&\sum_{m=0}^{15}\left(\frac{-1}{c_m}\right)\left(\frac{2}{c_m}\right)\\
=&\sum_{m=0}^{15}\left(\frac{-1}{c_m}\right)\left(\frac{c_m}{2}\right)\\
=&\begin{cases}2(-1)^{\frac{c_0-1}{2}}\left(\left(\frac{c_0}{2}\right)-\left(\frac{c_0-6}{2}\right)-\left(\frac{c_0-2}{2}\right)+\left(\frac{c_0-4}{2}\right)\right) & \text{if } c_0 \text{ is odd,}\\ 2(-1)^{\frac{c_0}{2}-1}\left[\left(\frac{c_0-2^{n-6}-4t-1}{2}\right)-\left(\frac{c_0-2^{n-6}-4t-3}{2}\right)\right. & \text{if } c_0 \text{ is even}\\ \left.+\left(\frac{c_0-2^{n-6}-4t-5}{2}\right)-\left(\frac{c_0-2^{n-6}-4t-7}{2}\right)\right] & \end{cases}\\
=&0.
\end{aligned}$$

Thus, $N_{D,d}(2^n)=0$ for $n\geq 8$.

For the cases that only one $m_i \equiv 2 \pmod 4$, the process is the same.

2.4.6 Case 2(i)(a)

Proof of Proposition 2.8 in **Case 2(i)(a)**. Recall the assumptions: $p|f$, $p \nmid d$ and $p \nmid D_0$ with p odd.

Since we have $p \nmid d$, we have

$$\sum_{n=0}^{\infty}\frac{(-1)^k N_{D,d}(p^n)}{p^{nk}}=\sum_{n=0}^{\infty}\frac{\left(\frac{d}{p}\right)^n N_{Dd}(p^n)}{p^{nk}}.$$

Thus in this part of the sub-case, we have to prove

$$\sum_{n=0}^{\infty} \frac{\left(\frac{d}{p}\right)^n N_{Dd}(p^n)}{p^{nk}} = \frac{1-p^{-2k}}{\left(1-\left(\frac{D_0}{p}\right)p^{-k}\right)\left(1-\left(\frac{d}{p}\right)p^{-k}\right)} \frac{1}{(p^e)^{2k-1}} \left(\sigma_{2k-1}(p^e) - \left(\frac{D_0}{p}\right) p^{k-1}\sigma_{2k-1}(p^{e-1})\right). \tag{2.17}$$

We need to compute $N_{Dd}(p^n) = v(p^n)$. We write $f = p^e m$ with $e \geq 1$ and $p \nmid m$. Then, $Dd = D_0 p^{2e} m^2 d$. In this part of the sub-case, we will prove the claims:

I. $N_{Dd}(p^{2n}) = N_{Dd}(p^{2n+1}) = p^n$ for $0 \leq n \leq e-1$.

II. $N_{Dd}(p^{2e}) = p^e$.

III. For $n \geq 2e+1$, $N_{Dd}(p^n) = \begin{cases} 0 & \text{if } \left(\frac{D_0 d}{p}\right) = -1, \\ 2p^e & \text{if } \left(\frac{D_0 d}{p}\right) = 1. \end{cases}$

Then, if $\left(\frac{D_0 d}{p}\right) = -1$, i.e., $\left(\frac{D_0}{p}\right) = -\left(\frac{d}{p}\right)$, comparing two sides of the identity (2.17), we have

$$\begin{aligned}
L.H.S. = \sum_{n=0}^{\infty} \frac{(-1)^k N_{D,d}(p^n)}{p^{nk}} &= \sum_{n=0}^{\infty} \frac{\left(\frac{d}{p}\right)^n N_{Dd}(p^n)}{p^{nk}} \\
&= 1 + \frac{\left(\frac{d}{p}\right)}{p^k} + \frac{p}{p^{2k}} + \frac{\left(\frac{d}{p}\right)p}{p^{3k}} + \frac{p^2}{p^{4k}} + \frac{\left(\frac{d}{p}\right)p^2}{p^{5k}} + \cdots \\
&\quad + \frac{p^{e-1}}{p^{(2e-2)k}} + \frac{\left(\frac{d}{p}\right)p^{e-1}}{p^{(2e-1)k}} + \frac{p^e}{p^{2ek}} \\
&= 1 + \frac{\left(\frac{d}{p}\right)}{p^k} + \frac{1}{p^{2k-1}} + \frac{\left(\frac{d}{p}\right)}{p^{2k-1+k}} + \frac{1}{p^{2(2k-1)}} + \frac{\left(\frac{d}{p}\right)}{p^{2(2k-1)+k}} + \cdots \\
&\quad + \frac{1}{p^{(e-1)(2k-1)}} + \frac{\left(\frac{d}{p}\right)}{p^{(e-1)(2k-1)+k}} + \frac{1}{p^{e(2k-1)}} \\
&= 1 + \frac{1}{p^{2k-1}} + \frac{1}{p^{2(2k-1)}} + \cdots + \frac{1}{p^{(e-1)(2k-1)}} + \frac{1}{p^{e(2k-1)}} \\
&\quad + \left(\frac{d}{p}\right) p^{-k} \left(1 + \frac{1}{p^{2k-1}} + \frac{1}{p^{2(2k-1)}} + \cdots + \frac{1}{p^{(e-1)(2k-1)}}\right) \\
&= \frac{1}{p^{2(2k-1)}} \left(1 + p^{2k-1} + p^{2(2k-1)} + \cdots + p^{(e-1)(2k-1)} + p^{e(2k-1)}\right) \\
&\quad + \left(\frac{d}{p}\right) p^{-k} \frac{1}{p^{(e-1)(2k-1)}} \left(1 + p^{2k-1} + p^{2(2k-1)} + \cdots + p^{(e-1)(2k-1)}\right) \\
&= \frac{1}{p^{e(2k-1)}} \left(\sigma_{2k-1}(p^e) + \left(\frac{d}{p}\right) p^{-k}\sigma_{2k-1}(p^{e-1})p^{2k-1}\right) \\
&= \frac{1}{p^{e(2k-1)}} \left(\sigma_{2k-1}(p^e) + \left(\frac{d}{p}\right) p^{k-1}\sigma_{2k-1}(p^{e-1})\right).
\end{aligned}$$

$$\begin{aligned}R.H.S. =&\frac{1-p^{-2k}}{\left(1-\left(\frac{D_0}{p}\right)p^{-k}\right)\left(1-\left(\frac{d}{p}\right)p^{-k}\right)}\frac{1}{(p^e)^{2k-1}}\left(\sigma_{2k-1}(p^e)-\left(\frac{D_0}{p}\right)p^{k-1}\sigma_{2k-1}(p^{e-1})\right)\\
=&\ \frac{1}{(p^e)^{2k-1}}\left(\sigma_{2k-1}(p^e)+\left(\frac{d}{p}\right)p^{k-1}\sigma_{2k-1}(p^{e-1})\right)\\
=&\ L.H.S.\end{aligned}$$

Now, if $\left(\frac{D_0 d}{p}\right)=1$, i.e., $\left(\frac{D_0}{p}\right)=\left(\frac{d}{p}\right)$, comparing two sides of the identity (2.17), we have

$$\begin{aligned}L.H.S. =&\sum_{n=0}^{\infty}\frac{(-1)^k N_{D,d}(p^n)}{p^{nk}}\\
=&\sum_{n=0}^{\infty}\frac{\left(\frac{d}{p}\right)^n N_{Dd}(p^n)}{p^{nk}}\\
=&1+\frac{\left(\frac{d}{p}\right)}{p^k}+\frac{p}{p^{2k}}+\frac{\left(\frac{d}{p}\right)p}{p^{3k}}+\frac{p^2}{p^{4k}}+\frac{\left(\frac{d}{p}\right)p^2}{p^{5k}}+\cdots\\
&+\frac{p^{e-1}}{p^{(2e-2)k}}+\frac{\left(\frac{d}{p}\right)p^{e-1}}{p^{(2e-1)k}}+\frac{p^e}{p^{2ek}}+\frac{\left(\frac{d}{p}\right)2p^e}{p^{(2e+1)k}}+\frac{2p^e}{p^{(2e+2)k}}+\cdots\\
=&\frac{1}{p^{e(2k-1)}}\left(\sigma_{2k-1}(p^e)+\left(\frac{d}{p}\right)p^{k-1}\sigma_{2k-1}(p^{e-1})\right)+\frac{\frac{2\left(\frac{d}{p}\right)p^e}{p^{(2e+1)k}}}{1-\left(\frac{d}{p}\right)p^{-k}}\\
=&\frac{\left(\sigma_{2k-1}(p^e)+\left(\frac{d}{p}\right)p^{k-1}\sigma_{2k-1}(p^{e-1})\right)}{p^{e(2k-1)}}+\frac{2\left(\frac{d}{p}\right)p^{e-2ek}}{p^k-\left(\frac{d}{p}\right)}\\
=&\frac{\left(p^k-\left(\frac{d}{p}\right)\right)\left(\sigma_{2k-1}(p^e)+\left(\frac{d}{p}\right)p^{k-1}\sigma_{2k-1}(p^{e-1})\right)+2\left(\frac{d}{p}\right)}{p^{e(2k-1)}\left(p^k-\left(\frac{d}{p}\right)\right)}\\
=&\frac{p^k\sigma_{2k-1}(p^e)-\left(\frac{d}{p}\right)\sigma_{2k-1}(p^e)+\left(\frac{d}{p}\right)p^{2k-1}\sigma_{2k-1}(p^{e-1})-p^{k-1}\sigma_{2k-1}(p^{e-1})+2\left(\frac{d}{p}\right)}{p^{e(2k-1)}(p^k-(\frac{d}{p}))}\\
=&\frac{p^k\sigma_{2k-1}(p^e)-p^{k-1}\sigma_{2k-1}(p^{e-1})+\left(\frac{d}{p}\right)(p^{2k-1}\sigma_{2k-1}(p^{e-1})-\sigma_{2k-1}(p^e)+2)}{p^{e(2k-1)}\left(p^k-\left(\frac{d}{p}\right)\right)}\\
=&\frac{p^k\sigma_{2k-1}(p^e)-p^{k-1}\sigma_{2k-1}(p^{e-1})+\left(\frac{d}{p}\right)}{p^{e(2k-1)}\left(p^k-\left(\frac{d}{p}\right)\right)}.\end{aligned}$$

$$
\begin{aligned}
R.H.S. =& \frac{1-p^{-2k}}{\left(1-\left(\frac{D_0}{p}\right)p^{-k}\right)\left(1-\left(\frac{d}{p}\right)p^{-k}\right)}\frac{1}{(p^e)^{2k-1}}\left(\sigma_{2k-1}(p^e)-\left(\frac{D_0}{p}\right)p^{k-1}\sigma_{2k-1}(p^{e-1})\right)\\
&= \frac{1+\left(\frac{d}{p}\right)p^{-k}}{1-\left(\frac{d}{p}\right)p^{-k}}\frac{\sigma_{2k-1}(p^e)-\left(\frac{d}{p}\right)p^{k-1}\sigma_{2k-1}(p^{e-1})}{(p^e)^{2k-1}}\\
&= \frac{\left(p^k+\left(\frac{d}{p}\right)\right)\left(\sigma_{2k-1}(p^e)-\left(\frac{d}{p}\right)p^{k-1}\sigma_{2k-1}(p^{e-1})\right)}{(p^e)^{2k-1}\left(p^k-\left(\frac{d}{p}\right)\right)}\\
&= \frac{p^k\sigma_{2k-1}(p^e)+(\frac{d}{p})\sigma_{2k-1}(p^e)-\left(\frac{d}{p}\right)p^{2k-1}\sigma_{2k-1}(p^{e-1})-p^{k-1}\sigma_{2k-1}(p^{e-1})}{(p^e)^{2k-1}\left(p^k-\left(\frac{d}{p}\right)\right)}\\
&= \frac{p^k\sigma_{2k-1}(p^e)-p^{k-1}\sigma_{2k-1}(p^{e-1})+\left(\frac{d}{p}\right)\left(\sigma_{2k-1}(p^e)-p^{2k-1}\sigma_{2k-1}(p^{e-1})\right)}{(p^e)^{2k-1}\left(p^k-\left(\frac{d}{p}\right)\right)}\\
&= \frac{p^k\sigma_{2k-1}(p^e)-p^{k-1}\sigma_{2k-1}(p^{e-1})+\left(\frac{d}{p}\right)}{(p^e)^{2k-1}\left(p^k-\left(\frac{d}{p}\right)\right)}\\
&= L.H.S.
\end{aligned}
$$

as required. □

Proof of Claim I and II. First of all, the equation $f(b) = b^2 - Dd \equiv 0 \pmod{p}$ has only one solution $b = 0$ since $p|D$. Thus, $N_{Dd}(p) = 1$. Now $f'(b) = 2b \equiv 0 \pmod{p}$ if and only if p divides b. We have $p|0$ and $(0)^2 - Dd \equiv 0 \pmod{p^2}$. Thus, 0 is lifted and the equation $b^2 - Dd \equiv 0 \pmod{p^2}$ has the solution set $\{t_1 p\}_{t_1=0}^{t_1=p-1}$. Thus, $N_{Dd}(p^2) = p$.

Now, we claim that for $1 \le n \le e$, the equation $b^2 - Dd \equiv 0 \pmod{p^{2n}}$ has the solution set $\{t_n p^n + t_{n+1}p^{n+1} + \cdots + t_{2n-1}p^{2n-1}\}$ with $t_i \in \{0, ..., p-1\}$.

If $e = 1$, then we have $n = 1$ and the claim is true. Thus, assume $e \ge 2$. We will prove by induction for $1 \le n \le e-1$. We have proved the first case when $n = 1$. Consider the equation $b^2 - Dd \equiv 0 \pmod{p^{2n+1}}$. Write $f = mp^e$ with $p \nmid m$. We see that

$$
\begin{aligned}
&(t_n p^n + t_{n+1}p^{n+1} + \cdots + t_{2n-1}p^{2n-1})^2 - D_0 p^{2e} m^2 d \equiv 0 \pmod{p^{2n+1}} \\
\Longleftrightarrow & p^{2n}(t_n + t_{n+1}p + \cdots + t_{2n-1}p^{n-1})^2 - D_0 p^{2e} m^2 d \equiv 0 \pmod{p^{2n+1}} \\
\Longleftrightarrow & (t_n + t_{n+1}p + \cdots + t_{2n-1}p^{n-1})^2 - D_0 p^{2e-2n} m^2 d \equiv 0 \pmod{p} \\
\Longleftrightarrow & t_n^2 - D_0 p^{2e-2n} m^2 d \equiv 0 \pmod{p} \\
\Longleftrightarrow & t_n^2 \equiv 0 \pmod{p} \\
\Longleftrightarrow & t_n = 0.
\end{aligned}
$$

Thus, the solutions $\{t_{n+1}p^{n+1} + \cdots + t_{2n-1}p^{2n-1}\}$ with $t_i \in \{0, ..., p-1\}$ are lifted. The equation $b^2 - Dd \equiv 0 \pmod{p^{2n+1}}$ has the solution set $\{t_{n+1}p^{n+1} + \cdots + t_{2n-1}p^{2n-1} + t_{2n}p^{2n}\}$ with $t_i \in \{0, ..., p-1\}$.

Now, consider the equation $b^2 - Dd \equiv 0 \pmod{p^{2n+2}}$. We see that

$$
\begin{aligned}
&(t_{n+1}p^{n+1} + t_{n+2}p^{n+2} \cdots + t_{2n-1}p^{2n-1} + t_{2n}p^{2n})^2 - D_0 p^{2e} m^2 d \equiv 0 \pmod{p^{2n+2}} \\
\Longleftrightarrow & p^{2n+2}(t_{n+1} + t_{n+2}p \cdots + t_{2n}p^{n-1})^2 - D_0 p^{2e} m^2 d \equiv 0 \pmod{p^{2n+2}} \\
\Longleftrightarrow & - D_0 p^{2e} m^2 d \equiv 0 \pmod{p^{2n+2}},
\end{aligned}
$$

which is always true since $2e \geq 2n+2$. Thus, the equation $b^2 - Dd \equiv 0 \pmod{p^{2n+2}}$ has the solution set $\{t_{n+1}p^{n+1} + \cdots + t_{2n-1}p^{2n-1} + t_{2n}p^{2n} + t_{2n+1}p^{2n+1}\}$ with $t_i \in \{0, ..., p-1\}$. The induction process shows that $N_{Dd}(p^{2n}) = N_{Dd}(p^{2n+1}) = p^n$ for $1 \leq n \leq e-1$ and $N_{Dd}(p^{2e}) = p^e$. $\square$

Proof of Claim III. We just show that the equation $b^2 - Dd \equiv 0 \pmod{p^{2e}}$ has the solution set $\{t_e p^e + t_{e+1}p^{e+1} + \cdots + t_{2e-1}p^{2e-1}\}$. Now, for the equation $b^2 - Dd \equiv 0 \pmod{p^{2e+1}}$, we see that

$$
\begin{aligned}
&(t_e p^e + t_{e+1}p^{e+1} + \cdots + t_{2e-1}p^{2e-1})^2 - Dd \equiv 0 \pmod{p^{2e+1}} \\
\Longleftrightarrow & p^{2e}(t_e + t_{e+1}p + \cdots + t_{2e-1}p^{e-1})^2 - D_0 p^{2e} m^2 d \equiv 0 \pmod{p^{2e+1}} \\
\Longleftrightarrow & (t_e + t_{e+1}p + \cdots + t_{2e-1}p^{e-1})^2 - D_0 m^2 d \equiv 0 \pmod{p} \\
\Longleftrightarrow & t_e^2 - D_0 m^2 d \equiv 0 \pmod{p} \\
\Longleftrightarrow & \left(\frac{D_0 d}{p}\right) = 1.
\end{aligned}
$$

Thus, if $\left(\frac{D_0 d}{p}\right) = 1$, the solutions $\pm(t_e p^e + t_{e+1}p^{e+1} + \cdots + t_{2e-1}p^{2e-1})$ (with a specific $t_e \neq 0$) is lifted and the equation $b^2 - Dd \equiv 0 \pmod{p^{2e+1}}$ has the solution set $\{\pm(t_e p^e + t_{e+1}p^{e+1} + \cdots +$

$t_{2e-1}p^{2e-1} + t_{2e}p^{2e})\}$ with $t_{e+1}, ..., t_{2e} \in \{0, ..., p-1\}$. Thus,

$$N_{Dd}(p^{2e+1}) = \begin{cases} 0 & \text{if } \left(\frac{D_0 d}{p}\right) = -1, \\ 2p^e & \text{if } \left(\frac{D_0 d}{p}\right) = 1. \end{cases}$$

So, if $\left(\frac{D_0 d}{p}\right) = 1$, we can look at $N_{Dd}(p^{2e+2})$. Now,

$$\begin{aligned}
&(t_e p^e + t_{e+1}p^{e+1} + \cdots + t_{2e}p^{2e})^2 - Dd \equiv 0 \pmod{p^{2e+2}} \\
\Longleftrightarrow &(t_e + t_{e+1}p + \cdots + t_{2e}p^e)^2 p^{2e} - D_0 p^{2e} m^2 d \equiv 0 \pmod{p^{2e+2}} \\
\Longleftrightarrow &(t_e + t_{e+1}p + \cdots + t_{2e}p^e)^2 - D_0 m^2 d \equiv 0 \pmod{p^2} \\
\Longleftrightarrow &(t_e + t_{e+1}p)^2 - D_0 m^2 d \equiv 0 \pmod{p^2} \\
\Longleftrightarrow &t_e^2 + 2t_e t_{e+1}p - D_0 m^2 d \equiv 0 \pmod{p^2} \\
\Longleftrightarrow &\frac{t_e^2 - D_0 m^2 d}{p} + 2t_e t_{e+1} \equiv 0 \pmod{p} \quad \text{ since } t_e^2 - D_0 m^2 d \equiv 0 \pmod{p}.
\end{aligned}$$

Since it is just a linear equation in t_{e+1} with $p \nmid 2t_e$, there is a unique t_{e+1} that will satisfy the equation. Thus, the solutions with a specific t_{e+1} are lifted and the equation $b^2 - Dd \equiv 0 \pmod{p^{2e+2}}$ has the solution set $\{\pm(t_e p^e + t_{e+1}p^{e+1} + \cdots + t_{2e-1}p^{2e-1} + t_{2e}p^{2e}) + t_{2e+1}p^{2e+1}\}$ with $t_{e+2}, ..., t_{2e+1} \in \{0, ..., p-1\}$. Thus, $N_{Dd}(p^{2e+2}) = 2p^e$.

Again, we write the solution set as $\{\pm(t_e p^e + t_{e+1}p^{e+1} + \cdots + t_{2e-1}p^{2e-1} + t_{2e}p^{2e} + t_{2e+1}p^{2e+1})\}$. Now,

$$\begin{aligned}
&(t_e p^e + t_{e+1}p^{e+1} + \cdots + t_{2e+1}p^{2e+1})^2 - Dd \equiv 0 \pmod{p^{2e+3}} \\
\Longleftrightarrow &(t_e + t_{e+1}p + \cdots + t_{2e}p^e)^2 p^{2e} - D_0 p^{2e} m^2 d \equiv 0 \pmod{p^{2e+3}} \\
\Longleftrightarrow &(t_e + t_{e+1}p + \cdots + t_{2e}p^e)^2 - D_0 m^2 d \equiv 0 \pmod{p^3} \\
\Longleftrightarrow &(t_e + t_{e+1}p + t_{e+2}p^2)^2 - D_0 m^2 d \equiv 0 \pmod{p^3} \\
\Longleftrightarrow &t_e^2 + 2t_e t_{e+1}p + t_{e+1}^2 p^2 + 2t_e t_{e+2}p^2 - D_0 m^2 d \equiv 0 \pmod{p^3} \\
\Longleftrightarrow &\frac{t_e^2 + 2t_e t_{e+1}p - D_0 m^2 d}{p^2} + t_{e+1}^2 + 2t_e t_{e+2} \equiv 0 \pmod{p}.
\end{aligned}$$

Again it is just a linear equation in t_{e+2} with $p \nmid 2t_e$. There is a unique t_{e+2} that will satisfy the equation. Thus, the solutions with a specific t_{e+2} are lifted and the equation $b^2 - Dd \equiv 0 \pmod{p^{2e+3}}$ has the solution set $\{\pm(t_e p^e + t_{e+1}p^{e+1} + \cdots + t_{2e}p^{2e} + t_{2e+1}p^{2e+1} + t_{2e+2}p^{2e+2})\}$ with $t_{e+3}, ..., t_{2e+2} \in \{0, ..., p-1\}$. Thus, $N_{Dd}(p^{2e+3}) = 2p^e$. We see that this pattern will continue and thus $N_{Dd}(p^n) = 2p^e$ for all $n \geq 2e+1$. □

2.4.7 Case 2(i)(b)

Proof of Proposition 2.8 in **Case 2(i)(b)**. Recall the assumptions: $p|f$, $p \nmid d$ and $p \nmid D_0$ with $p = 2$.

Similar to the previous part of the sub-case, since we have $2 \nmid d$, we have

$$\sum_{n=0}^{\infty} \frac{(-1)^k N_{D,d}(2^n)}{2^{nk}} = \sum_{n=0}^{\infty} \frac{\left(\frac{d}{2}\right)^n N_{Dd}(2^n)}{2^{nk}}.$$

Thus in this part of the sub-case, we have to prove

$$\sum_{n=0}^{\infty} \frac{\left(\frac{d}{2}\right)^n N_{Dd}(2^n)}{2^{nk}} = \frac{1-2^{-2k}}{\left(1-\left(\frac{D_0}{2}\right)2^{-k}\right)\left(1-\left(\frac{d}{2}\right)2^{-k}\right)} \frac{1}{(2^e)^{2k-1}} \left(\sigma_{2k-1}(2^e) - \left(\frac{D_0}{2}\right) 2^{k-1}\sigma_{2k-1}(2^{e-1})\right). \tag{2.18}$$

We need to compute $N_{Dd}(2^n) = \frac{1}{2}v(2^{n+2})$. We write $f = 2^e m$ with $e \geq 1$ and $2 \nmid m$. Then, $Dd = D_0 2^{2e} m^2 d$.

In this part of the sub-case, we will prove the same claims as the previous part:

I. $N_{Dd}(2^{2n}) = N_{Dd}(2^{2n+1}) = p^n$ for $0 \leq n \leq e-1$.

II. $N_{Dd}(2^{2e}) = 2^e$.

III. For $n \geq 2e+1$, $N_{Dd}(2^n) = \begin{cases} 0 & \text{if } \left(\frac{D_0 d}{2}\right) = -1, \\ 2 \cdot 2^e & \text{if } \left(\frac{D_0 d}{2}\right) = 1. \end{cases}$

Then, the rest is exactly the same as the previous part of the sub-case and thus the equation (2.18) is true. □

Proof of Claim I and II. We first assume $e \geq 2$. Consider the equation

$$\begin{aligned} b^2 - Dd \equiv 0 \pmod{4 \cdot 2} &\Longleftrightarrow b^2 - D_0 2^{2e} m^2 d \equiv 0 \pmod{8} \\ &\Longleftrightarrow b^2 \equiv 0 \pmod{8} \\ &\Longleftrightarrow b = 0 \text{ or } 4. \end{aligned}$$

Thus, the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2}$ has the solution set $\{2^2 t\}_{t=0}^{t=1}$. Therefore, $N_{Dd}(2) = 1$.

For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^2}$, we see that

$$\begin{aligned} (2^2 t)^2 - Dd \equiv 0 \pmod{4 \cdot 2^2} &\Longleftrightarrow 2^4 t^2 - D_0 2^2 m^2 d \equiv 0 \pmod{2)^4} \\ &\Longleftrightarrow 0 \equiv 0 \pmod{4}, \end{aligned}$$

which is always true. Thus both solutions are lifted and the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^2}$ has the solution set $\{2^2t, 2^2t + 2^3\}_{t=0}^{t=1} = \{2^2t, 2^2(t+2)\}_{t=0}^{t=1} = \{2^2t\}_{t=0}^{t=3}$. Thus, $N_{Dd}(2^2) = 2$.

Now, we claim that the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2n}}$ has the solution set $\{2^{n+1}t\}_{t=0}^{t=2^{n+1}-1}$ for $1 \leq n \leq e-1$. To see this, note that

$$\begin{aligned} b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2n}} &\iff b^2 - D_0 2^{2e} m^2 d \equiv 0 \pmod{2^{2n+2}} \\ &\iff b^2 \equiv 0 \pmod{2^{2n+2}} \text{ since } 2e \geq 2n+2 \\ &\iff t \text{ is a multiple of } 2^{n+1}. \end{aligned}$$

Thus, the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2n}}$ has the solution set $\{2^{n+1}t\}_{t=0}^{t=2^{n+1}-1}$. This shows $N_{Dd}(2^{2n}) = 2^n$ for $1 \leq n \leq e-1$.

For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2n+1}}$ for $1 \leq n \leq e-2$, we see that

$$\begin{aligned} (2^{n+1}t)^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2n+1}} &\iff 2^{2n+2}t^2 - D_0 2^{2e} m^2 d \equiv 0 \pmod{2}^{2n+3} \\ &\iff 2^{2n+2}t^2 \equiv 0 \pmod{2}^{2n+3} \text{ since } 2e \geq 2n+4 \\ &\iff t^2 \equiv 0 \pmod{2} \\ &\iff t \text{ is even.} \end{aligned}$$

Thus, the solutions with even t are lifted. The equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2n+1}}$ for $1 \leq n \leq e-2$ has the solution set

$$\begin{aligned} \{2^{n+1}t, 2^{n+1}t + 2^{2n+2}\}_{t=0,2,\ldots,2^{n+1}-2} &= \{2^{n+2}t, 2^{n+2}t + 2^{2n+2}\}_{t=0}^{t=2^n-1} \\ &= \{2^{n+2}t, 2^{n+2}(t + 2^n)\}_{t=0}^{t=2^n-1} \\ &= \{2^{n+2}t\}_{t=0}^{t=2^{n+1}-1}. \end{aligned}$$

This shows $N_{Dd}(2^{2n+1}) = 2^n$ for $1 \leq n \leq e-2$.

Now, to find $N_{Dd}(2^{2n+1})$ for $n = e-1$, i.e., $N_{Dd}(2^{2e-1})$, for all $e \geq 1$, we consider the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e-1}}$. Recall that the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e-2}}$ has the solution set $\{2^e t\}_{t=0}^{t=2^e-1}$. We see that

$$\begin{aligned} (2^e t)^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e-1}} &\iff 2^{2e}t^2 - D_0 2^{2e} m^2 d \equiv 0 \pmod{2}^{2e+1} \\ &\iff t^2 - D_0 m^2 d \equiv 0 \pmod{2} \\ &\iff t^2 - 1 \equiv 0 \pmod{2} \\ &\iff t \text{ is odd.} \end{aligned}$$

Thus, the solutions with odd t are lifted and the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e-1}}$ has the solution set

$$\begin{aligned}\{2^e t, 2^e t + 2^{2e}\}_{t=1,3,\ldots,2^e-1} &= \{2^{e+1}t + 2^e, 2^{e+1}t + 2^e + 2^{2e}\}_{t=0}^{t=2^{e-1}-1} \\ &= \{2^{e+1}t + 2^e, 2^{e+1}(t + 2^{e-1}) + 2^e\}_{t=0}^{t=2^{e-1}-1} \\ &= \{2^{e+1}t + 2^e\}_{t=0}^{t=2^e-1} \\ &= \{2^e(2t+1)\}_{t=0}^{t=2^e-1}.\end{aligned}$$

This shows $N_{Dd}(2^{2e-1}) = 2^{e-1}$.

Now, in order to find $N_{Dd}(2^{2e-1})$, we consider the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e}}$. We see that

$$\begin{aligned}[2^e(2t+1)]^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e}} &\Longleftrightarrow 2^{2e}(2t+1)^2 - D_0 2^{2e} m^2 d \equiv 0 \ (\mathrm{mod}\ 2)^{2e+2} \\ &\Longleftrightarrow (2t+1)^2 - D_0 m^2 d \equiv 0 \pmod 4 \\ &\Longleftrightarrow 1 - D_0 m^2 d \equiv 0 \pmod 4,\end{aligned}$$

which is always true. Thus, all solutions are lifted. The equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e}}$ has the solution set

$$\begin{aligned}\{2^e(2t+1), 2^e(2t+1) + 2^{2e+1}\}_{t=0}^{t=2^e-1} &= \{2^e(2t+1), 2^e(2t+1+2^{e+1})\}_{t=0}^{t=2^e-1} \\ &= \{2^e(2t+1), 2^e[(2(t+2^e)+1]\}_{t=0}^{t=2^e-1} \\ &= \{2^e(2t+1)\}_{t=0}^{t=2^{e+1}-1}.\end{aligned}$$

This shows $N_{Dd}(2^{2e}) = 2^e$. □

Proof of Claim III. Now we look at the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+1}}$ and consider

$$\begin{aligned}[2^e(2t+1)]^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+1}} &\Longleftrightarrow 2^{2e}(2t+1)^2 - D_0 2^{2e} m^2 d \equiv 0 \pmod{2^{2e+3}} \\ &\Longleftrightarrow (2t+1)^2 - D_0 m^2 d \equiv 0 \pmod{2^3} \\ &\Longleftrightarrow 4t^2 + 4t + 1 - D_0 m^2 d \equiv 0 \pmod{2^3}.\end{aligned}$$

Note that $D_0 m^2 d \equiv 1$ or $5 \pmod 8$. If $D_0 m^2 d \equiv 5 \pmod 8$, we have

$$\begin{aligned}4t^2 + 4t + 1 - D_0 m^2 d \equiv 0 \pmod{2^3} &\Longleftrightarrow 4t^2 + 4t \equiv 4 \pmod 8 \\ &\Longleftrightarrow t^2 + t \equiv 1 \pmod 2 \\ &\Longleftrightarrow t(t+1) \equiv 1 \pmod 2,\end{aligned}$$

which is never true. Thus, no solution is lifted. We have $N_{Dd}(2^{2e+1}) = 0$ and $N_{Dd}(2^n) = 0$ for $n \geq 2e+1$.

If $D_0 m^2 d \equiv 1 \pmod 8$, we have

$$\begin{aligned} 4t^2 + 4t + 1 - D_0 m^2 d \equiv 0 \pmod{2^3} &\Longleftrightarrow 4t^2 + 4t \equiv 0 \pmod 8 \\ &\Longleftrightarrow t^2 + t \equiv 0 \pmod 2 \\ &\Longleftrightarrow t(t+1) \equiv 0 \pmod 2, \end{aligned}$$

which is always true. Thus, all solutions are lifted and the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+1}}$ has the solution set

$$\begin{aligned} \{2^e(2t+1), 2^e(2t+1) + 2^{2e+2}\}_{t=0}^{t=2^{e+1}-1} &= \{2^e(2t+1), 2^e(2t+1+2^{e+2})\}_{t=0}^{t=2^{e+1}-1} \\ &= \{2^e(2t+1), 2^e[(2(t+2^{e+1})+1]\}_{t=0}^{t=2^{e+1}-1} \\ &= \{2^e(2t+1)\}_{t=0}^{t=2^{e+2}-1}. \end{aligned}$$

This shows $N_{Dd}(2^{2e+1}) = 2^{e+1}$.

To continue the process, we first rewrite the above solution set. Note that

$$\begin{aligned} \{2^e(2t+1)\}_{t=0}^{t=2^{e+2}-1} &= \{2^e(4t+1), 2^e(4t+3)\}_{t=0}^{t=2^{e+1}-1} \\ &= \{2^e(4t+1), 2^e(4t+3) - 2^{2e+3}\}_{t=0}^{t=2^{e+1}-1} \\ &= \{2^e(4t+1), -2^e(-4t-3+2^{e+3})\}_{t=0}^{t=2^{e+1}-1} \\ &= \{2^e(4t+1), -2^e[4(2^{e+1}-t)-3]\}_{t=0}^{t=2^{e+1}-1} \\ &= \{2^e(4t+1), -2^e[4(2^{e+1}-1-t)+1]\}_{t=0}^{t=2^{e+1}-1} \\ &= \{2^e(4t+1), -2^e[4(2^{e+1}-1-t)+1]\}_{t=0}^{t=2^{e+1}-1} \\ &= \{2^e(4t+1), -2^e(4t+1)\}_{t=0}^{t=2^{e+1}-1} \\ &= \{\pm 2^e(4t+1)\}_{t=0}^{t=2^{e+1}-1}. \end{aligned}$$

For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+2}}$, we see that

$$\begin{aligned} [2^e(4t+1)]^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+2}} &\Longleftrightarrow 2^{2e}(4t+1)^2 - D_0 2^{2e} m^2 d \equiv 0 \pmod{2^{2e+4}} \\ &\Longleftrightarrow (4t+1)^2 - D_0 m^2 d \equiv 0 \pmod{2^4} \\ &\Longleftrightarrow 8t + 1 - D_0 m^2 d \equiv 0 \pmod{16} \\ &\Longleftrightarrow 8t + 1 \equiv D_0 m^2 d \pmod{16}. \end{aligned}$$

If $D_0m^2d \equiv 1 \pmod{2^4}$, we have

$$\begin{aligned} 8t+1 \equiv D_0m^2d \pmod{16} &\Longleftrightarrow 8t \equiv 0 \pmod{16} \\ &\Longleftrightarrow t \equiv 0 \pmod{2} \\ &\Longleftrightarrow t \text{ is even.} \end{aligned}$$

Thus, the solutions with even t are lifted and the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+2}}$ has the solution set $\{\pm 2^e(2^3t+1)\}_{t=0}^{t=2^{e+1}-1}$.

If $D_0m^2d \equiv 2^3+1 \pmod{2^4}$, we have

$$\begin{aligned} 8t+1 \equiv D_0m^2d \pmod{16} &\Longleftrightarrow 8t \equiv 8 \pmod{16} \\ &\Longleftrightarrow t \equiv 1 \pmod{2} \\ &\Longleftrightarrow t \text{ is odd.} \end{aligned}$$

Thus, the solutions with odd t are lifted and the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+2}}$ has the solution set $\{\pm 2^e(2^3t+2^2+1)\}_{t=0}^{t=2^{e+1}-1}$.

For each case, $N_{Dd}(2^{2e+2}) = 2^{e+1}$. We can generalize the above phenomenon to the claim: For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+1+n}}$, $n \geq 1$, if $D_0m^2d \equiv 2^3r+1 \equiv 2^{n+3}$ for some $r \in \{0, 1, ..., 2^n-1\}$, it has the solution set $\{\pm 2^e(2^{n+2}t+2^2s+1)\}_{t=0}^{t=2^{e+1}-1}$ for some $s \in \{0, 1, ..., 2^n-1\}$ with $(2^2s+1)^2 \equiv 2^3r+1$.

We have just proved the case with $n = 1$. We can use an induction argument to prove this as in Case 1(iv)(b). This will prove Claim III. □

2.4.8 Case 2(ii)(a)

Proof of Proposition 2.8 in **Case 2(ii)(a)**. Recall the assumptions: $p|f$, $p \nmid d$ and $p|D_0$ with p odd.

We still have $p \nmid d$, so we have

$$\sum_{n=0}^{\infty} \frac{(-1)^k N_{D,d}(p^n)}{p^{nk}} = \sum_{n=0}^{\infty} \frac{\left(\frac{d}{p}\right)^n N_{Dd}(p^n)}{p^{nk}}.$$

Thus in this part of the sub-case, we have to prove the same identity

$$\sum_{n=0}^{\infty} \frac{\left(\frac{d}{p}\right)^n N_{Dd}(p^n)}{p^{nk}} = \frac{1-p^{-2k}}{\left(1-\left(\frac{D_0}{p}\right)p^{-k}\right)\left(1-\left(\frac{d}{p}\right)p^{-k}\right)} \frac{1}{(p^e)^{2k-1}} \left(\sigma_{2k-1}(p^e) - \left(\frac{D_0}{p}\right)p^{k-1}\sigma_{2k-1}(p^{e-1})\right). \tag{2.19}$$

We need to compute $N_{Dd}(p^n) = v(p^n)$. We write $f = p^em$ with $e \geq 1$ and $p \nmid m$. Then, $Dd = D_0p^{2e}m^2d$.

In this part of the sub-case, we will prove the claims:

I. $N_{Dd}(p^{2n}) = N_{Dd}(p^{2n+1}) = p^n$ for $0 \le n \le e$.

II. $N_{Dd}(p^n) = 0$ for $n \ge 2e+2$.

Thus, comparing two sides of the identity (2.19) we have

$$\begin{aligned}
L.H.S. =& \sum_{n=0}^{\infty} \frac{(-1)^k N_{D,d}(p^n)}{p^{nk}} \\
=& \sum_{n=0}^{\infty} \frac{\left(\frac{d}{p}\right)^n N_{Dd}(p^n)}{p^{nk}} \\
=& 1 + \frac{\left(\frac{d}{p}\right)}{p^k} + \frac{p}{p^{2k}} + \frac{\left(\frac{d}{p}\right)p}{p^{3k}} + \frac{p^2}{p^{4k}} + \frac{\left(\frac{d}{p}\right)p^2}{p^{5k}} + \cdots + \frac{p^e}{p^{2ek}} + \frac{\left(\frac{d}{p}\right)p^e}{p^{(2e+1)k}} \\
=& 1 + \frac{\left(\frac{d}{p}\right)}{p^k} + \frac{1}{p^{2k-1}} + \frac{\left(\frac{d}{p}\right)}{p^{2k-1+k}} + \frac{1}{p^{2(2k-1)}} + \frac{\left(\frac{d}{p}\right)}{p^{2(2k-1)+k}} + \cdots + \frac{1}{p^{e(2k-1)}} + \frac{\left(\frac{d}{p}\right)}{p^{e(2k-1)+k}} \\
=& 1 + \frac{1}{p^{2k-1}} + \frac{1}{p^{2(2k-1)}} + \cdots + \frac{1}{p^{(e-1)(2k-1)}} + \frac{1}{p^{e(2k-1)}} \\
& + \left(\frac{d}{p}\right) p^{-k} \left(1 + \frac{1}{p^{2k-1}} + \frac{1}{p^{2(2k-1)}} + \cdots + \frac{1}{p^{e(2k-1)}}\right).
\end{aligned}$$

$$\begin{aligned}
R.H.S. =& \frac{1-p^{-2k}}{\left(1-\left(\frac{D_0}{p}\right)p^{-k}\right)\left(1-\left(\frac{d}{p}\right)p^{-k}\right)} \frac{1}{(p^e)^{2k-1}} \left(\sigma_{2k-1}(p^e) - \left(\frac{D_0}{p}\right) p^{k-1} \sigma_{2k-1}(p^{e-1})\right) \\
=& \left(1 + \left(\frac{d}{p}\right)p^{-k}\right) \frac{\sigma_{2k-1}(p^e)}{(p^e)^{2k-1}} \\
=& \left(1 + \frac{\left(\frac{d}{p}\right)}{p^k}\right)\left(1 + \frac{1}{p^{2k-1}} + \cdots + \frac{1}{p^{e(2k-1)}}\right) \\
=& L.H.S.
\end{aligned}$$

as required. □

Proof of Claim I. Note that everything follow as Case 2(i)(a) up to the point that the equation $b^2 - Dd \equiv 0 \pmod{p^{2e}}$ has the solution set $\{t_e p^e + t_{e+1}p^{e+1} + \cdots + t_{2e-1}p^{2e-1}\}$ with $t_i \in \{0, 1, ..., p-1\}$. Therefore, we have $N_{Dd}(p^{2n}) = N_{Dd}(p^{2n+1}) = p^n$ for $0 \le n \le e-1$ and $N_{Dd}(p^{2e}) = p^e$. To find

$N_{Dd}(p^{2e+1})$, we consider the equation $b^2 - Dd \equiv 0 \pmod{p^{2e+1}}$. We see that

$$
\begin{aligned}
&(t_e p^e + t_{e+1}p^{e+1} + \cdots + t_{2e-1}p^{2e-1})^2 - Dd \equiv 0 \pmod{p^{2e+1}} \\
\Longleftrightarrow & p^{2e}(t_e + t_{e+1}p + \cdots + t_{2e-1}p^{e-1})^2 - D_0 p^{2e} m^2 d \equiv 0 \pmod{p^{2e+1}} \\
\Longleftrightarrow & p^{2e}(t_e + t_{e+1}p + \cdots + t_{2e-1}p^{e-1})^2 \equiv 0 \pmod{p^{2e+1}} \\
\Longleftrightarrow & (t_e + t_{e+1}p + \cdots + t_{2e-1}p^{e-1})^2 \equiv 0 \pmod{p} \\
\Longleftrightarrow & t_e^2 \equiv 0 \pmod{p} \\
\Longleftrightarrow & t_e = 0.
\end{aligned}
$$

Thus, the solutions $\{t_e p^e + t_{e+1}p^{e+1} + \cdots + t_{2e-1}p^{2e-1}\}$ are lifted and the equation $b^2 - Dd \equiv 0 \pmod{p^{2e+1}}$ has the solution set $\{t_e p^e + t_{e+1}p^{e+1} + \cdots + t_{2e-1}p^{2e-1} + t_{2e}p^{2e}\}$ with $t_i \in \{0, 1, ..., p-1\}$. That shows $N_{Dd}(p^{2e+1}) = p^e$. Thus, Claim I is proved. □

Proof of Claim II. For equation $b^2 - Dd \equiv 0 \pmod{p^{2e+2}}$, we see that

$$
\begin{aligned}
&(t_{e+1}p^{e+1} + t_{e+2}p^{e+2} + \cdots + t_{2e}p^{2e})^2 - Dd \equiv 0 \pmod{p^{2e+2}} \\
\Longleftrightarrow & p^{2e+2}(t_{e+1} + t_{e+2}p + \cdots + t_{2e}p^{e-1})^2 - D_0 p^{2e} m^2 d \equiv 0 \pmod{p^{2e+2}} \\
\Longleftrightarrow & - D_0 p^{2e} m^2 d \equiv 0 \pmod{p^{2e+2}} \\
\Longleftrightarrow & - D_0 m^2 d \equiv 0 \pmod{p^2} \\
\Longleftrightarrow & - \frac{D_0}{p} m^2 d \equiv 0 \pmod{p},
\end{aligned}
$$

which is always false. So no solution is lifted and the equation $b^2 - Dd \equiv 0 \pmod{p^{2e+2}}$ has no solution. Thus, $N_{Dd}(p^{2e+2}) = 0$ and $N_{Dd}(p^n) = 0$ for $n \geq 2e+2$. □

2.4.9 Case 2(ii)(b)

Proof of Proposition 2.8 in **Case 2(ii)(b)**. Recall the assumptions: $p|f$, $p \nmid d$ and $p|D_0$ with $p = 2$.

Similar to the previous part of the sub-case, since we have $2 \nmid d$, we have

$$
\sum_{n=0}^{\infty} \frac{(-1)^k N_{D,d}(2^n)}{2^{nk}} = \sum_{n=0}^{\infty} \frac{\left(\frac{d}{2}\right)^n N_{Dd}(2^n)}{2^{nk}}.
$$

Thus in this part of the sub-case, we have to prove

$$
\sum_{n=0}^{\infty} \frac{\left(\frac{d}{2}\right)^n N_{Dd}(2^n)}{2^{nk}} = \frac{1 - 2^{-2k}}{\left(1 - \left(\frac{D_0}{2}\right) 2^{-k}\right)\left(1 - \left(\frac{d}{2}\right) 2^{-k}\right)} \frac{1}{(2^e)^{2k-1}} \left(\sigma_{2k-1}(2^e) - \left(\frac{D_0}{2}\right) 2^{k-1} \sigma_{2k-1}(2^{e-1})\right). \tag{2.20}
$$

We need to compute $N_{Dd}(2^n) = \frac{1}{2}v(2^{n+2})$. We write $f = 2^e m$ with $e \geq 1$ and $2 \nmid m$. Then, $Dd = D_0 2^{2e} m^2 d$.

In this part of the sub-case, we will prove the same claims as the previous part:

I. $N_{Dd}(2^{2n}) = N_{Dd}(2^{2n+1}) = 2^n$ for $0 \leq n \leq e$.

II. $N_{Dd}(2^n) = 0$ for $n \geq 2e+2$.

Thus, the rest is exactly the same as the previous part of the sub-case and the identity (2.20) is true. □

Proof of Claim I. Everything follows exactly as in Case 2(i)(b) up to the point that the equation $b^2 - Dd \equiv 0 \pmod{2^{2e}}$ has the solution set $\{2^e t\}_{t=0}^{t=2^e-1}$. Thus, we have $N_{Dd}(2^{2n}) = N_{Dd}(2^{2n+1}) = 2^n$ for $0 \leq n \leq e-2$ and $N_{Dd}(2^{2e-2}) = 2^{e-1}$.

To determine $N_{Dd}(2^{2e-1})$, we consider the equation $b^2 - Dd \equiv 0 \pmod{2^{2e+1}}$. We see that

$$\begin{aligned}(2^e t)^2 - Dd \equiv 0 \pmod{2^{2e+1}} &\Longleftrightarrow 2^{2e}t^2 - 2^{2e+2}m_2 m^2 d \equiv 0 \pmod{2^{2e+2}}\\ &\Longleftrightarrow 2^{2e}t^2 \equiv 0 \pmod{2^{2e+2}}\\ &\Longleftrightarrow t^2 \equiv 0 \pmod{2^2}\\ &\Longleftrightarrow t \text{ is even.}\end{aligned}$$

Thus, all solutions are lifted and the equation $b^2 - Dd \equiv 0 \pmod{2^{2e+1}}$ has the solution set

$$\begin{aligned}\{2^e t, 2^e t + 2^{2e}\}_{t=0,2,\ldots,2^e-2} &= \{2^{e+1}t, 2^{e+1}t + 2^{2e})\}_{t=0}^{t=2^{e-1}-1}\\ &= \{2^e t, 2^{e+1}(t + 2^{e-1})\}_{t=0}^{t=2^{e-1}-1}\\ &= \{2^{e+1}t\}_{t=0}^{t=2^e-1}.\end{aligned}$$

This shows $N(2^{2e-1}) = 2^{e-1}$.

To determine $N_{Dd}(2^{2e})$, we consider the equation $b^2 - Dd \equiv 0 \pmod{2^{2e+2}}$. We see that

$$\begin{aligned}(2^{e+1}t)^2 - Dd \equiv 0 \pmod{2^{2e+2}} &\Longleftrightarrow 2^{2e+2}t^2 - 2^{2e+2}m_2 m^2 d \equiv 0 \pmod{2^{2e+2}}\\ &\Longleftrightarrow 0 \equiv 0 \pmod{2^{2e+2}},\end{aligned}$$

which is always true. Thus, all solutions are lifted and the equation $b^2 - Dd \equiv 0 \pmod{2^{2e+2}}$ has the solution set

$$\begin{aligned}\{2^{e+1}t, 2^{e+1}t + 2^{2e+1})\}_{t=0}^{t=2^e-1} &= \{2^{e+1}t, 2^{e+1}(t + 2^e)\}_{t=0}^{t=2^e-1}\\ &= \{2^{e+1}t\}_{t=0}^{t=2^{e+1}-1}.\end{aligned}$$

This shows $N(2^{2e}) = 2^e$.

To determine $N_{Dd}(2^{2e+1})$, we consider the equation $b^2 - Dd \equiv 0 \pmod{2^{2e+3}}$. We see that

$$\begin{aligned}
(2^{e+1}t)^2 - Dd \equiv 0 \pmod{2^{2e+3}} &\Longleftrightarrow 2^{2e+2}t^2 - 2^{2e+2}m_2m^2d \equiv 0 \pmod{2^{2e+3}} \\
&\Longleftrightarrow t^2 - m_2m^2d \equiv 0 \pmod{2} \\
&\Longleftrightarrow t^2 - m_2 \equiv 0 \pmod{2}
\end{aligned}$$

If $m_2 \equiv 2 \pmod{4}$, then we have

$$t^2 \equiv 0 \pmod{2} \Longleftrightarrow t \text{ is even.}$$

Thus, the solutions with even t are lifted and the equation $b^2 - Dd \equiv 0 \pmod{2^{2e+3}}$ has the solution set

$$\begin{aligned}
\{2^{e+1}t, 2^{e+1}t + 2^{2e+2}\}_{t=0,2,\ldots,2^{e+1}-2} &= \{2^{e+2}t, 2^{e+2}t + 2^{2e+2})\}_{t=0}^{t=2^e-1} \\
&= \{2^{e+2}t, 2^{e+2}(t + 2^e)\}_{t=0}^{t=2^e-1} \\
&= \{2^{e+2}t\}_{t=0}^{t=2^{e+1}-1}.
\end{aligned}$$

This shows $N(2^{2e+1}) = 2^e$.

If $m_2 \equiv 3 \pmod{4}$, then we have

$$t^2 - 1 \equiv 0 \pmod{2} \Longleftrightarrow t \text{ is odd.}$$

Thus, the solutions with odd t are lifted and the equation $b^2 - Dd \equiv 0 \pmod{2^{2e+3}}$ has the solution set

$$\begin{aligned}
\{2^{e+1}t, 2^{e+1}t + 2^{2e+2}\}_{t=1,3,\ldots,2^{e+1}-1} &= \{2^{e+2}t + 2^{e+1}, 2^{e+2}t + 2^{e+1} + 2^{2e+2})\}_{t=0}^{t=2^e-1} \\
&= \{2^{e+1}(2t+1), 2^{e+1}(2t + 1 + 2^{e+1})\}_{t=0}^{t=2^e-1} \\
&= \{2^{e+1}(2t+1), 2^{e+1}[2(t + 2^e) + 1]\}_{t=0}^{t=2^e-1} \\
&= \{2^{e+1}(2t+1)\}_{t=0}^{t=2^{e+1}-1}.
\end{aligned}$$

This shows $N(2^{2e+1}) = 2^e$. □

Proof of Claim II. To determine $N_{Dd}(2^{2e+2})$, we consider the equation $b^2 - Dd \equiv 0 \pmod{2^{2e+4}}$. If $m_2 \equiv 2 \pmod 4$, we see that

$$\begin{aligned}(2^{e+2}t)^2 - Dd \equiv 0 \pmod{2^{2e+4}} &\iff 2^{2e+4}t^2 - 2^{2e+2}m_2m^2d \equiv 0 \pmod{2^{2e+4}} \\ &\iff -m_2m^2d \equiv 0 \pmod{2^2} \\ &\iff -\frac{m_2}{2}m^2d \equiv 0 \pmod 2,\end{aligned}$$

which is never true. Thus, $N(2^{2e+2}) = 0$ and $N(2^n) = 0$ for all $n \geq 2e+2$.

If $m_2 \equiv 3 \pmod 4$, we see that

$$\begin{aligned}[2^{e+1}(2t+1)]^2 - Dd \equiv 0 \pmod{2^{2e+4}} &\iff 2^{2e+2}(2t+1)^2 - 2^{2e+2}m_2m^2d \equiv 0 \pmod{2^{2e+4}} \\ &\iff (2t+1)^2 - m_2m^2d \equiv 0 \pmod{2^2} \\ &\iff 1 - m_2m^2d \equiv 0 \pmod 4 \\ &\iff 1 - 3 \equiv 0 \pmod 4 \\ &\iff -2 \equiv 0 \pmod 4,\end{aligned}$$

which is never true. Thus, $N(2^{2e+2}) = 0$ and $N(2^n) = 0$ for all $n \geq 2e+2$. □

2.4.10 Case 2(iii)(a)

Proof of Proposition 2.8 in **Case 2(iii)(a)**. Recall the assumptions: $p|f$, $p|d$ and $p \nmid D_0$ with p odd.

Since we have $p|d$ here, we have to compute $N_{D,d}(p^n)$ explicitly again.

We make the following claims in this part of the sub-case:

I. $N_{D,d}(p^{2n+1}) = 0$ for $0 \leq n \leq e-1$.

II. $N_{D,d}(p^{2n}) = (-1)^k(p^n - p^{n-1})$ for $1 \leq n \leq e$.

III. $N_{D,d}(p^{2e+1}) = (-1)^k \left(\frac{D_0}{p}\right) p^e$.

IV. $N_{D,d}(p^n) = 0$ for $n \geq 2e+2$.

Thus, we have that

$$\sum_{n=0}^{\infty}\frac{(-1)^k N_{D,d}(p^n)}{p^{nk}}$$
$$=1+\frac{p-1}{p^{2k}}+\frac{p^2-p}{p^{4k}}+\frac{p^3-p^2}{p^{6k}}+\cdots+\frac{p^e-p^{e-1}}{p^{2ek}}+\frac{\left(\frac{D_0}{p}\right)p^e}{p^{(2e+1)k}}$$
$$=1+\frac{1}{p^{2k-1}}+\frac{1}{p^{2(2k-1)}}+\cdots+\frac{1}{p^{e(2k-1)}}-\left(\frac{1}{p^{2k}}+\frac{1}{p^{4k-1}}+\frac{1}{p^{6k-2}}+\cdots+\frac{1}{p^{2ek-e+1}}\right)+\frac{\left(\frac{D_0}{p}\right)p^e}{p^{(2e+1)k}}$$
$$=\frac{\sigma_{2k-1}(p^e)}{p^{e(2k-1)}}-\frac{p^{(e-1)(2k-1)}+p^{(e-2)(2k-1)}+\cdots+p^{2k-1}+1}{p^{e(2k-1)+1}}+\frac{\left(\frac{D_0}{p}\right)p^e}{p^{(2e+1)k}}$$
$$=\frac{\sigma_{2k-1}(p^e)}{p^{e(2k-1)}}-\frac{\sigma_{2k-1}(p^{e-1})}{p^{e(2k-1)+1}}+\frac{\left(\frac{D_0}{p}\right)}{p^{e(2k-1)+k}}$$
$$=\frac{p^k\sigma_{2k-1}(p^e)+\left(\frac{D_0}{p}\right)\sigma_{2k-1}(p^e)-\left(\frac{D_0}{p}\right)p^{2k-1}\sigma_{2k-1}(p^{e-1})-p^{k-1}\sigma_{2k-1}(p^{e-1})}{p^{e(2k-1)+k}}$$
$$=\frac{p^k+\left(\frac{D_0}{p}\right)}{p^k}\cdot\frac{\sigma_{2k-1}(p^e)-\left(\frac{D_0}{p}\right)p^{k-1}\sigma_{2k-1}(p^{e-1})}{p^{e(2k-1)}}$$
$$=\left(1+\left(\frac{D_0}{p}\right)p^{-k}\right)\frac{1}{p^{e(2k-1)}}\left(\sigma_{2k-1}(p^e)-\left(\frac{D_0}{p}\right)p^{k-1}\sigma_{2k-1}(p^{e-1})\right)$$
$$=\frac{1-p^{-2k}}{\left(1-\left(\frac{D_0}{p}\right)p^{-k}\right)\left(1-\left(\frac{d}{p}\right)p^{-k}\right)}\frac{1}{(p^e)^{2k-1}}\left(\sigma_{2k-1}(p^e)-\left(\frac{D_0}{p}\right)p^{k-1}\sigma_{2k-1}(p^{e-1})\right)$$

as required. □

Proof of Claim I and II. Note that in this case the solutions to $b^2-Dd\equiv 0 \pmod{p^n}$ for any n are the same as those in Case 2(ii)(a). For $n=1$, there is only one solution $b=0$ to the equation $b^2-Dd\equiv 0 \pmod p$. On the other hand, the equation $b^2-Dd\equiv 0 \pmod 4$ always has two solutions. Thus, there is only one solution to $b^2-Dd\equiv 0 \pmod 4)p$ with $0\le b\le 2p^2-1$ and it looks like $t'p$ for some integer t'. Then,

$$N_{D,d}(p)=\sum_{\substack{0\le b\le 2p-1\\ b^2\equiv Dd \pmod{4p}}}\chi_d\left(\left[-p,b,\frac{Dd-b^2}{4p}\right]\right)=\chi_d\left(\left[-p,t'p,\frac{Dd-(t'p)^2}{4p}\right]\right)=0.$$

We have seen that the solution set to $b^2-Dd\equiv 0 \pmod{p^2}$ is $\{t_1p\}$ with $t_1\in\{0,1,...,p-1\}$. Then the solution set to $b^2-Dd\equiv 0 \pmod{4p^2}$ with $0\le b\le 2p-1$ looks like $\{t_1p+m_{t_1}p^2\}$ with $t_1\in\{0,1,...,p-1\}$ and m_{t_1} fixed. Let $c_{t_1}=\frac{Dd-(t_1p+m_{t_1}p^2)^2}{4p^2}$. Thus,

$$
\begin{aligned}
N_{D,d}(p^2) &= \sum_{\substack{0 \le b \le 2p-1 \\ b^2 \equiv Dd \pmod{4p}}} \chi_d([-p^2, b, c]) \\
&= \sum_{t_1=0}^{p-1} \chi_d([-p^2, t_1 p + m_{t_1} p^2, c_{t_1}]) \\
&= \begin{cases} \sum_{t_1=0}^{p-1} \left(\frac{\frac{d}{p}}{-p^2}\right)\left(\frac{p}{c_{t_1}}\right) & \text{if } p \equiv 1 \pmod 4, \\ \sum_{t_1=0}^{p-1} \left(\frac{-\frac{d}{p}}{-p^2}\right)\left(\frac{-p}{c_{t_1}}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases} \\
&= \begin{cases} (-1)^k \sum_{t_1=0}^{p-1} \left(\frac{p}{c_{t_1}}\right) & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{k+1} \sum_{t_1=0}^{p-1} \left(\frac{-p}{c_{t_1}}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases} \\
&= \begin{cases} (-1)^k \sum_{t_1=0}^{p-1} \left(\frac{c_{t_1}}{p}\right) & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{k+1} \sum_{t_1=0}^{p-1} \left(\frac{c_{t_1}}{p}\right) & \text{if } p \equiv 3 \pmod 4. \end{cases}
\end{aligned}
$$

Then, we have

$$
\begin{aligned}
\sum_{t_1=0}^{p-1} \left(\frac{c_{t_1}}{p}\right) &= \sum_{t_1=0}^{p-1} \left(\frac{\frac{Dd-(t_1 p + m_{t_1} p^2)^2}{4p^2}}{p}\right) \\
&= \sum_{t_1=0}^{p-1} \left(\frac{\frac{Dd-(t_1 p + m_{t_1} p^2)^2}{p^2}}{p}\right) \\
&= \sum_{t_1=0}^{p-1} \left(\frac{\frac{Dd}{p^2} - (t_1 + m_{t_1} p)^2}{p}\right) \\
&= \sum_{t_1=0}^{p-1} \left(\frac{-t_1^2}{p}\right) \ \text{(since } p | \frac{Dd}{p^2}) \\
&= \left(\frac{-1}{p}\right) \sum_{t_1=0}^{p-1} \left(\frac{t_1^2}{p}\right) \\
&= \left(\frac{-1}{p}\right)(p-1).
\end{aligned}
$$

Thus, $N_{D,d}(p^2) = (-1)^k(p-1)$.

For $2 \le n \le e$, the solution set for $b^2 - Dd \equiv 0 \pmod{p^{2n-1}}$ is $\{t_n p^n + t_{n+1} p^{n+1} + \cdots + t_{2n-2} p^{2n-2}\}$ with $t_n, t_{n+1}, ..., t_{2n-2} \in \{0, 1, ..., p-1\}$. Thus, the equation $b^2 - Dd \equiv 0 \pmod{4p^{2n-1}}$ with $0 \le b \le 2p^{2n-1}$ also has p^{n-1} solutions, $b_t = t_n p^n + t_{n+1} p^{n+1} + \cdots + t_{2n-2} p^{2n-2} + m_t p^{2n-1}$ for some fixed integer m_t. Let $c_t = \frac{Dd-b_t^2}{4p^{2n-1}}$. Thus,

$$N_{D,d}(p^{2n-1}) = \sum_{t=0}^{p^{n-1}} \chi_d([-p^{2n-1}, b_t, c_t])$$
$$= \begin{cases} \sum_{t=1}^{p^{n-1}} \left(\frac{\frac{d}{p}}{-p^{2n-1}}\right)\left(\frac{p}{c_t}\right) & \text{if } p \equiv 1 \pmod 4, \\ \sum_{t=1}^{p^{n-1}} \left(\frac{-\frac{d}{p}}{-p^{2n-1}}\right)\left(\frac{-p}{c_t}\right) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

However,

$$\begin{aligned} c_t &= \frac{Dd - (t_n p^n + t_{n+1}p^{n+1} + \cdots + t_{2n-2}p^{2n-2} + m_t p^{2n-1})^2}{4p^{2n-1}} \\ &= \frac{D_0 p^{2e} m^2 d - (t_n + t_{n+1}p + \cdots + t_{2n-2}p^{n-2} + m_t p^{n-1})^2 p^{2n}}{4p^{2s-1}} \\ &= \frac{D_0 p^{2e-2n+1} m^2 d - (t_n + t_{n+1}p + \cdots + t_{2n-2}p^{n-2} + m_t p^{n-1})^2 p}{4}. \end{aligned}$$

Therefore p divides c_t and $N_{D,d}(p^{2n-1}) = 0$ for $2 \leq n \leq e$.

For $1 \leq n \leq e$, the solution set for $b^2 - Dd \equiv 0 \pmod{p^{2n}}$ is $\{t_n p^n + t_{n+1}p^{n+1} + \cdots + t_{2n-1}p^{2n-1}\}$ with $t_n, t_{n+1}, ..., t_{2n-1} \in \{0, 1, ..., p-1\}$. Thus, the equation $b^2 - Dd \equiv 0 \pmod{4p^{2n}}$ has p^n solutions, $b_t = t_n p^n + t_{n+1}p^{n+1} + \cdots + t_{2n-1}p^{2n-1} + m_t p^{2n}$, with m_t fixed. Let $c_t = \frac{Dd-b_t^2}{4p^{2n}}$. Then,

$$N_{D,d}(p^{2n}) = \sum_{t=0}^{p^n} \chi_d([-p^{2n}, b_t, c_t])$$
$$= \begin{cases} \sum_{t=1}^{p^n} \left(\frac{\frac{d}{p}}{-p^{2n}}\right)\left(\frac{p}{c_t}\right) & \text{if } p \equiv 1 \pmod 4, \\ \sum_{t=1}^{p^n} \left(\frac{-\frac{d}{p}}{-p^{2n}}\right)\left(\frac{-p}{c_t}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases}$$
$$= \begin{cases} (-1)^k \sum_{t=1}^{p^n} \left(\frac{c_t}{p}\right) & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{k+1} \sum_{t=1}^{p^n} \left(\frac{c_t}{p}\right) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Now, we have

$$\begin{aligned}
\sum_{t=1}^{p^n}\left(\frac{c_t}{p}\right) &= \sum_{t_n=0}^{p-1}\sum_{t_{n+1}=0}^{p-1}\cdots\sum_{t_{2n-1}=0}^{p-1}\left(\frac{\frac{Dd-(t_np^n+t_{n+1}p^{n+1}+\cdots+t_{2n-1}p^{2s-1}+m_tp^{2n})^2}{4p^{2n}}}{p}\right)\\
&= \sum_{t_n=0}^{p-1}\sum_{t_{n+1}=0}^{p-1}\cdots\sum_{t_{2n-1}=0}^{p-1}\left(\frac{\frac{D_0p^{2e}m^2d-(t_n+t_{n+1}p+\cdots+t_{2n-1}p^{n-1}+m_tp^n)^2p^{2n}}{p^{2n}}}{p}\right)\\
&= \sum_{t_n=0}^{p-1}\sum_{t_{n+1}=0}^{p-1}\cdots\sum_{t_{2n-1}=0}^{p-1}\left(\frac{D_0p^{2e-2n}m^2d-(t_n+t_{n+1}p+\cdots+t_{2n-1}p^{n-1}+m_tp^n)^2}{p}\right)\\
&= \sum_{t_n=0}^{p-1}\sum_{t_{n+1}=0}^{p-1}\cdots\sum_{t_{2n-1}=0}^{p-1}\left(\frac{-t_n^2}{p}\right) \qquad (\text{since } p|D_0p^{2e-2n}m^2d)\\
&= \left(\frac{-1}{p}\right)\sum_{t_n=0}^{p-1}\sum_{t_{n+1}=0}^{p-1}\cdots\sum_{t_{2n-1}=0}^{p-1}\left(\frac{t_n^2}{p}\right)\\
&= \left(\frac{-1}{p}\right)\sum_{t_{n+1}=0}^{p-1}\cdots\sum_{t_{2n-1}=0}^{p-1}\sum_{t_n=0}^{p-1}\left(\frac{t_n^2}{p}\right)\\
&= \left(\frac{-1}{p}\right)\sum_{t_{n+1}=0}^{p-1}\cdots\sum_{t_{2n-1}=0}^{p-1}(p-1)\\
&= \left(\frac{-1}{p}\right)p^{n-1}(p-1)\\
&= \left(\frac{-1}{p}\right)(p^n-p^{n-1}).
\end{aligned}$$

Thus, $N_{D,d}(p^{2n}) = (-1)^k(p^n - p^{n-1})$. □

Proof of Claim III. Recall that the equation $b^2-Dd \equiv 0 \pmod{p^{2e+1}}$ has the solution set $\{t_{e+1}p^{e+1}+t_{e+2}p^{e+2}+\cdots+t_{2e}p^{2e}\}$ with $t_i \in \{0,1,...,p-1\}$. Thus, the equation $b^2-Dd \equiv 0 \pmod{4p^{2e+1}}$ with $0 \le b \le 2p^{2e+1}$ has p^e solutions, $b_t = t_{e+1}p^{e+1}+t_{e+2}p^{e+2}+\cdots+t_{2e}p^{2e}+m_tp^{2e+1}$ for some fixed integer m_t. Let $c_t = \frac{Dd-b_t^2}{4p^{2e+1}}$. Then,

$$
\begin{aligned}
N_{D,d}(p^{2e+1}) &= \sum_{t=0}^{p^e} \chi_d([-p^{2e+1}, b_t, c_t]) \\
&= \begin{cases} \sum_{t=1}^{p^e} \left(\frac{\frac{d}{p}}{-p^{2e+1}}\right)\left(\frac{p}{c_t}\right) & \text{if } p \equiv 1 \pmod 4, \\ \sum_{t=1}^{p^e} \left(\frac{-\frac{d}{p}}{-p^{2e+1}}\right)\left(\frac{-p}{c_t}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases} \\
&= \begin{cases} \left(\frac{\frac{d}{p}}{-p}\right) \sum_{t=1}^{p^e} \left(\frac{c_t}{p}\right) & \text{if } p \equiv 1 \pmod 4, \\ \left(\frac{-\frac{d}{p}}{-p}\right) \sum_{t=1}^{p^e} \left(\frac{c_t}{p}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases} \\
&= \begin{cases} (-1)^k \left(\frac{\frac{d}{p}}{p}\right) \sum_{t=1}^{p^e} \left(\frac{c_t}{p}\right) & \text{if } p \equiv 1 \pmod 4, \\ \left(\frac{-1}{p}\right)\left(\frac{\frac{d}{p}}{p}\right)\left(\frac{-\frac{d}{p}}{-1}\right) \sum_{t=1}^{p^e} \left(\frac{c_t}{p}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases} \\
&= \begin{cases} (-1)^k \left(\frac{\frac{d}{p}}{p}\right) \sum_{t=1}^{p^e} \left(\frac{c_t}{p}\right) & \text{if } p \equiv 1 \pmod 4, \\ (-1)^k \left(\frac{\frac{d}{p}}{p}\right) \sum_{t=1}^{p^e} \left(\frac{c_t}{p}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases} \\
&= (-1)^k \left(\frac{\frac{d}{p}}{p}\right) \sum_{t=1}^{p^e} \left(\frac{c_t}{p}\right).
\end{aligned}
$$

Then, we have

$$
\begin{aligned}
&\sum_{t=1}^{p^e} \left(\frac{c_t}{p}\right) \\
&= \sum_{t_{e+1}=0}^{p-1} \sum_{t_{e+2}=0}^{p-1} \cdots \sum_{t_{2e}=0}^{p-1} \left(\frac{\frac{Dd-(t_{e+1}p^{e+1}+t_{e+2}p^{e+2}+\cdots+t_{2e}p^{2e}+m_t p^{2e+1})^2}{4p^{2e+1}}}{p}\right) \\
&= \sum_{t_{e+1}=0}^{p-1} \sum_{t_{e+2}=0}^{p-1} \cdots \sum_{t_{2e}=0}^{p-1} \left(\frac{\frac{D_0 p^{2e} m^2 d-(t_{e+1}+t_{e+2}p+\cdots+t_{2e}p^{e-1}+m_t p^e)^2 p^{2e+2}}{p^{2e+1}}}{p}\right) \\
&= \sum_{t_{e+1}=0}^{p-1} \sum_{t_{e+2}=0}^{p-1} \cdots \sum_{t_{2e}=0}^{p-1} \left(\frac{D_0 m^2 \frac{d}{p} - (t_{e+1}+t_{e+2}p+\cdots+t_{2e}p^{e-1}+m_t p^e)^2 p}{p}\right) \\
&= \sum_{t_{e+1}=0}^{p-1} \sum_{t_{e+2}=0}^{p-1} \cdots \sum_{t_{2e}=0}^{p-1} \left(\frac{D_0 m^2 \frac{d}{p}}{p}\right) \\
&= \left(\frac{D_0 \frac{d}{p}}{p}\right) p^e.
\end{aligned}
$$

Thus, $N_{D,d}(p^{2e+1}) = (-1)^k \left(\frac{D_0}{p}\right) p^e$. □

Proof of Claim IV. As in Case 2(ii)(a), $b^2 - Dd \equiv 0 \pmod{p^n}$ for $n \geq 2e+2$ has no solution. Thus, $N_{D,d}(p^n) = 0$ for $n \geq 2e+2$. □

2.4.11 Case 2(iii)(b)

Proof of Proposition 2.8 in **Case 2(iii)(b)**. Recall the assumptions: $p|f$, $p|d$ and $p \nmid D_0$ with $p = 2$.

In this part of the sub-cases, we will prove the same claims as the previous part:

I. $N_{D,d}(2^{2n+1}) = 0$ for $0 \leq n \leq e-1$.

II. $N_{D,d}(2^{2n}) = (-1)^k(2^n - 2^{n-1})$ for $1 \leq n \leq e$.

III. $N_{D,d}(2^{2e+1}) = (-1)^k \left(\frac{D_0}{2}\right) 2^e$.

IV. $N_{D,d}(2^n) = 0$ for $n \geq 2e+2$.

Then the rest will be exactly the same as the previous part of the sub-cases. □

Proof of Claim I and II. The solutions to the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2n}}$ for all n in this case are the same as those in Case 2(ii)(b) except that for $n = 2e+1$, we switch m_2 to m_1.

Recall the the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2n+1}}$ for $0 \leq n \leq e-1$ has the solution set $\{2^{n+2}t\}_{t=0}^{t=2^{n+1}-1}$. Let $c_t = \frac{Dd-(2^{n+2}t)^2}{4 \cdot 2^{2n+1}}$. Then,

$$\begin{aligned}
N_{D,d}(2^{2n+1}) &= \sum_{\substack{0 \leq b \leq 2\cdot 2^{2n+1}-1 \\ b^2 \equiv Dd \pmod{4\cdot 2^{2^n+1}}}} \chi_d\left(\left[-2^{2n+1}, b, \frac{Dd-b^2}{4\cdot 2^{2n+1}}\right]\right) \\
&= \sum_{t=0}^{2^n-1} \chi_d([-2^{2n+1}, 2^{n+2}t, c_t]).
\end{aligned}$$

We have

$$\begin{aligned}
c_t &= \frac{Dd - (2^{n+2}t)^2}{2^{2n+3}} \\
&= \frac{D_0 2^{2e+2} m^2 m_1 - 2^{2n+4}t^2}{2^{2n+3}} \\
&= D_0 2^{2e-2n-1} m^2 m_1 - 2t^2.
\end{aligned}$$

Since $2e - 2n - 1 \geq 1$, $2|c_t$. Thus, $N_{D,d}(2^{2n+1}) = 0$ for $0 \leq n \leq e-1$.

Now, recall that the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2n}}$ for $1 \le n \le e$ has the solution set $\{2^{n+1}t\}_{t=0}^{t=2^{n+1}-1}$. Let $c_t = \frac{Dd-(2^{n+1}t)^2}{2^{2n+2}} = \frac{D_0 2^{2e} m^2 4 m_1 - 2^{2n+2} t^2}{2^{2n+2}} = D_0 m^2 m_1 2^{2e-2n} - t^2 = c_0 - t^2$. Thus,

$$\begin{aligned}
N_{D,d}(2^{2n}) &= \sum_{\substack{0 \le b \le 2(2^{2n})-1 \\ b^2 \equiv Dd \pmod{4 \cdot 2^{2n}}}} \chi_d\left(\left[-2^{2n}, b, \frac{Dd-b^2}{4 \cdot 2^{2n}}\right]\right) \\
&= \sum_{t=0}^{2^n-1} \chi_d([-2^{2n}, 2^{n+1}t, c_t]) \\
&= \begin{cases} \sum_{t=0}^{2^n-1} \left(\frac{-m_1}{-2^{2n}}\right)\left(\frac{-4}{c_t}\right) & \text{if } m_1 \equiv 3 \pmod 4, \\ \sum_{t=0}^{2^n-1} \left(\frac{\frac{m_1}{2}}{-2^{2n}}\right)\left(\frac{8}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4, \\ \sum_{t=0}^{2^n-1} \left(\frac{-\frac{m_1}{2}}{-2^{2n}}\right)\left(\frac{-8}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4 \end{cases} \\
&= \begin{cases} (-1)^{k+1} \sum_{t=0}^{2^n-1} \left(\frac{-4}{c_t}\right) & \text{if } m_1 \equiv 3 \pmod 4, \\ (-1)^{k} \sum_{t=0}^{2^n-1} \left(\frac{2}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4, \\ (-1)^{k+1} \sum_{t=0}^{2^n-1} \left(\frac{-2}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4. \end{cases}
\end{aligned}$$

First consider $n \neq e$. If $m_1 \equiv 3 \pmod 4$, we have

$$\begin{aligned}
N_{D,d}(2^{2n}) = (-1)^{k+1} \sum_{t=0}^{2^n-1} \left(\frac{-4}{c_t}\right) &= (-1)^{k+1} \sum_{t=1,3,\ldots,2^n-1} \left(\frac{-4}{c_t}\right) \\
&= (-1)^{k+1} \sum_{t=1,3,\ldots,2^n-1} \left(\frac{-1}{c_t}\right) \\
&= (-1)^{k+1} \sum_{t=1,3,\ldots,2^n-1} (-1)^{\frac{c_t-1}{2}} \\
&= (-1)^{k+1} \sum_{t=1,3,\ldots,2^n-1} (-1)^{\frac{c_0-t^2-1}{2}} \\
&= (-1)^{k+1} \sum_{t=1,3,\ldots,2^n-1} (-1)^{\frac{-t^2-1}{2}} \\
&= (-1)^{k+1} \sum_{t=1,3,\ldots,2^n-1} (-1)^{\frac{t^2+1}{2}} \\
&= (-1)^{k+1} \sum_{t=1,3,\ldots,2^n-1} (-1) \\
&= (-1)^{k+1}(-2^{n-1}) \\
&= (-1)^{k}(2^n - 2^{n-1}).
\end{aligned}$$

If $m_1 \equiv 2 \pmod 8$, we have

$$\begin{aligned}
N_{D,d}(2^{2n}) = (-1)^k \sum_{t=0}^{2^n-1} \left(\frac{2}{c_t}\right) &= (-1)^k \sum_{t=0}^{2^n-1} \left(\frac{c_t}{2}\right) \\
&= (-1)^k \sum_{t=1,3,\ldots,2^n-1} \left(\frac{c_t}{2}\right) \\
&= (-1)^k \sum_{t=1,3,\ldots,2^n-1} \left(\frac{c_0 - t^2}{2}\right) \\
&= (-1)^k \left(\frac{c_0 - 1}{2}\right) (2^{n-1}) \\
&= (-1)^k (2^{n-1}) \text{ since } 8 | c_0 \\
&= (-1)^k (2^n - 2^{n-1}).
\end{aligned}$$

If $m_1 \equiv 6 \pmod 8$, we have

$$\begin{aligned}
N_{D,d}(2^{2n}) = (-1)^{k+1} \sum_{t=0}^{2^n-1} \left(\frac{-2}{c_t}\right) &= (-1)^{k+1} \sum_{t=1,3,\ldots,2^n-1} \left(\frac{-2}{c_t}\right) \\
&= (-1)^{k+1} \sum_{t=1,3,\ldots,2^n-1} \left(\frac{-1}{c_t}\right) \left(\frac{2}{c_t}\right) \\
&= (-1)^{k+1} \sum_{t=1,3,\ldots,2^n-1} (-1) \left(\frac{c_t}{2}\right) \\
&= (-1)^{k} \sum_{t=1,3,\ldots,2^n-1} \left(\frac{c_t}{2}\right) \\
&= (-1)^k (2^n - 2^{n-1}).
\end{aligned}$$

Now consider $n = e$.
If $m_1 \equiv 3 \pmod 4$, we have

$$\begin{aligned}
N_{D,d}(2^{2n}) = (-1)^{k+1} \sum_{t=0,2,4,\ldots,2^n-2} \left(\frac{-4}{c_t}\right) &= (-1)^{k+1} \sum_{t=0,2,4,\ldots,2^n-2} \left(\frac{-1}{c_t}\right) \\
&= (-1)^{k+1} \sum_{t=0,2,4,\ldots,2^n-2} (-1)^{\frac{D_0 m^2 m_1 - t^2 - 1}{2}} \\
&= (-1)^{k+1} \sum_{t=0,2,4,\ldots,2^n-2} (-1) \\
&= (-1)^{k+1} (-2^{n-1}) \\
&= (-1)^k (2^n - 2^{n-1}).
\end{aligned}$$

If $m_1 \equiv 2 \pmod 8$, we have

$$\begin{aligned}
N_{D,d}(2^{2n}) &= (-1)^k \sum_{t=0}^{2^n-1} \left(\frac{2}{c_t}\right) \\
&= (-1)^k \sum_{t=0}^{2^n-1} \left(\frac{c_t}{2}\right) \\
&= (-1)^k \sum_{t=1,3,\ldots,2^n-1} \left(\frac{c_t}{2}\right) \\
&= (-1)^k \sum_{t=1,3,\ldots,2^n-1} \left(\frac{c_0 - t^2}{2}\right) \\
&= (-1)^k \left(\frac{c_0 - 1}{2}\right) (2^{n-1}) \\
&= (-1)^k (2^{n-1}) \text{ since } c_0 \equiv 2 \pmod 8 \\
&= (-1)^k (2^n - 2^{n-1}).
\end{aligned}$$

If $m_1 \equiv 6 \pmod 8$, it is exactly the same as before. □

Proof of Claim III. Recall that the equation $b^2 - Dd \equiv 0 \pmod{2^{2e+3}}$ has the solution set

$$\begin{cases} \{2^{e+2}t\}_{t=0}^{t=2^{e+1}-1} & \text{if } m_1 \equiv 2 \pmod 4, \\ \{2^{e+1}(2t+1)\}_{t=0}^{t=2^{e+1}-1} & \text{if } m_1 \equiv 3 \pmod 4. \end{cases}$$

First consider $m_1 \equiv 2 \pmod 4$. Let $c_t = \frac{Dd-(2^{e+2}t)^2}{2^{2e+3}} = D_0 m^2 \frac{m_1}{2} - 2t^2 = c_0 - 2t^2$. Then,

$$\begin{aligned}
N_{D,d}(2^{2e+1}) &= \sum_{t=0}^{2^e-1} \chi_d([-2^{2e+1}, 2^{e+2}t, c_t]) \\
&= \begin{cases} \sum_{t=0}^{2^e-1} \left(\frac{\frac{m_1}{2}}{-2^{2e+1}}\right) \left(\frac{8}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4, \\ \sum_{t=0}^{2^e-1} \left(\frac{-\frac{m_1}{2}}{-2^{2e+1}}\right) \left(\frac{-8}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4 \end{cases} \\
&= \begin{cases} (-1)^k \left(\frac{\frac{m_1}{2}}{2}\right) \sum_{t=0}^{2^e-1} \left(\frac{2}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4, \\ (-1)^{k+1} \left(\frac{\frac{m_1}{2}}{2}\right) \sum_{t=0}^{2^e-1} (-1)^{\frac{c_t-1}{2}} \left(\frac{2}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4. \end{cases}
\end{aligned}$$

First consider $\frac{m_1}{2} \equiv 1 \pmod 4$. If $\left(\frac{\frac{m_1}{2}}{2}\right) = \left(\frac{D_0}{2}\right)$, i.e., $\frac{m_1}{2} \equiv 1 \pmod 8$ and $D_0 \equiv 1 \pmod 8$ or $\frac{m_1}{2} \equiv 5 \pmod 8$ and $D_0 \equiv 5 \pmod 8$, then

$$\begin{aligned}\sum_{t=0}^{2^e-1}\left(\frac{c_t}{2}\right) = &\sum_{t=0}^{2^e-1}\left(\frac{D_0 m^2\frac{m_1}{2} - 2t^2}{2}\right)\\ =&2^{e-1}\left[\left(\frac{D_0 m^2\frac{m_1}{2}}{2}\right) + \left(\frac{D_0 m^2\frac{m_1}{2} - 2}{2}\right)\right]\\ =&2^{e-1}\left[\left(\frac{1}{2}\right) + \left(\frac{7}{2}\right)\right]\\ =&2^e.\end{aligned}$$

Thus, $N_{D,d}(2^{2e+1}) = (-1)^k\left(\frac{D_0}{2}\right)2^e$.

If $\left(\frac{\frac{m_1}{2}}{2}\right) \neq \left(\frac{D_0}{2}\right)$, i.e., $\frac{m_1}{2} \equiv 1 \pmod 8$ and $D_0 \equiv 5 \pmod 8$ or $\frac{m_1}{2} \equiv 5 \pmod 8$ and $D_0 \equiv 1 \pmod 8$, then

$$\begin{aligned}\sum_{t=0}^{2^e-1}\left(\frac{c_t}{2}\right) =&2^{e-1}\left[\left(\frac{D_0 m^2\frac{m_1}{2}}{2}\right) + \left(\frac{D_0 m^2\frac{m_1}{2} - 2}{2}\right)\right]\\ =&2^{e-1}\left[\left(\frac{5}{2}\right) + \left(\frac{3}{2}\right)\right]\\ =& - 2^e.\end{aligned}$$

Thus, we still have $N_{D,d}(2^{2e+1}) = (-1)^k\left(\frac{D_0}{2}\right)2^e$.

Now consider $\frac{m_1}{2} \equiv 3 \pmod 4$. If $\left(\frac{\frac{m_1}{2}}{2}\right) = \left(\frac{D_0}{2}\right)$, i.e., $\frac{m_1}{2} \equiv 3 \pmod 8$ and $D_0 \equiv 5 \pmod 8$ or $\frac{m_1}{2} \equiv 7 \pmod 8$ and $D_0 \equiv 1 \pmod 8$, then

$$\begin{aligned}\sum_{t=0}^{2^e-1}(-1)^{\frac{c_t-1}{2}}\left(\frac{c_t}{2}\right) &= \sum_{t=0}^{2^e-1}(-1)^{\frac{D_0 m^2\frac{m_1}{2}-2t^2-1}{2}}\left(\frac{D_0 m^2\frac{m_1}{2} - 2t^2}{2}\right)\\ &= \sum_{t=0}^{2^e-1}(-1)^{\frac{D_0 m^2\frac{m_1}{2}-1}{2}-t^2}\left(\frac{D_0 m^2\frac{m_1}{2} - 2t^2}{2}\right)\\ &= 2^{e-1}\left[(-1)^{\frac{D_0 m^2\frac{m_1}{2}-1}{2}}\left(\frac{D_0 m^2\frac{m_1}{2}}{2}\right) - (-1)^{\frac{D_0 m^2\frac{m_1}{2}-1}{2}}\left(\frac{D_0 m^2\frac{m_1}{2} - 2}{2}\right)\right]\\ &= 2^{e-1}\left[-\left(\frac{7}{2}\right) + \left(\frac{5}{2}\right)\right]\\ &= -2^e.\end{aligned}$$

Thus, $N_{D,d}(2^{2e+1}) = (-1)^k\left(\frac{D_0}{2}\right)2^e$.

If $\left(\frac{\frac{m_1}{2}}{2}\right) \neq \left(\frac{D_0}{2}\right)$, i.e., $\frac{m_1}{2} \equiv 3 \pmod 8$ and $D_0 \equiv 1 \pmod 8$ or $\frac{m_1}{2} \equiv 7 \pmod 8$ and $D_0 \equiv 5 \pmod 8$, then

$$\begin{aligned}\sum_{t=0}^{2^e-1}(-1)^{\frac{c_t-1}{2}}\left(\frac{c_t}{2}\right) &= 2^{e-1}\left[(-1)^{\frac{D_0m^2\frac{m_1}{2}-1}{2}}\left(\frac{D_0m^2\frac{m_1}{2}}{2}\right)-(-1)^{\frac{D_0m^2\frac{m_1}{2}-1}{2}}\left(\frac{D_0m^2\frac{m_1}{2}-2}{2}\right)\right]\\ &= 2^{e-1}\left[-\left(\frac{3}{2}\right)+\left(\frac{1}{2}\right)\right]\\ &= 2^e.\end{aligned}$$

Thus, we still have $N_{D,d}(2^{2e+1}) = (-1)^k\left(\frac{D_0}{2}\right)2^e$.

Now, we consider $m_1 \equiv 3 \pmod 4$. We have the solution set $\{2^{e+1}(2t+1)\}_{t=0}^{t=2^{e+1}-1}$. Let $c_t = \frac{Dd-[2^{e+1}(2t+1)]^2}{2^{2e+3}} = \frac{D_0m^2m_1-1}{2} - 2t^2 - 2t = c_0 - 2t^2 - 2t$. Thus, we have

$$\begin{aligned}N_{D,d}(2^{2e+1}) &= \sum_{t=0}^{2^e-1}\chi_d([-2^{2e+1}, 2^{e+1}(2t+1), c_t])\\ &= \sum_{t=0}^{2^e-1}\left(\frac{-m_1}{-2^{2e+1}}\right)\left(\frac{-4}{c_t}\right)\\ &=(-1)^{k+1}\left(\frac{m_1}{2}\right)\sum_{t=0}^{2^e-1}\left(\frac{-4}{c_t}\right)\\ &=(-1)^{k+1}\left(\frac{m_1}{2}\right)\sum_{t=0}^{2^e-1}\left(\frac{-1}{c_t}\right)\\ &=(-1)^{k+1}\left(\frac{m_1}{2}\right)\sum_{t=0}^{2^e-1}(-1)^{\frac{c_t-1}{2}}\\ &=(-1)^{k+1}\left(\frac{m_1}{2}\right)\sum_{t=0}^{2^e-1}(-1)^{\frac{\frac{D_0m^2m_1-1}{2}-2t^2-2t-1}{2}}\\ &=(-1)^{k+1}\left(\frac{m_1}{2}\right)\sum_{t=0}^{2^e-1}(-1)^{\frac{\frac{D_0m^2m_1-1}{2}-1}{2}}\\ &=(-1)^{k+1}\left(\frac{m_1}{2}\right)\cdot 2^e\cdot(-1)^{\frac{\frac{D_0m^2m_1-1}{2}-1}{2}}.\end{aligned}$$

If $\left(\frac{m_1}{2}\right) = \left(\frac{D_0}{2}\right)$, i.e., $m_1 \equiv 3 \pmod 8, D_0 \equiv 5 \pmod 8$ or $m_1 \equiv 7 \pmod 8, D_0 \equiv 1 \pmod 8$, then $(-1)^{\frac{\frac{D_0m^2m_1-1}{2}-1}{2}} = -1$.

If $\left(\frac{m_1}{2}\right) = -\left(\frac{D_0}{2}\right)$, i.e., $m_1 \equiv 3 \pmod 8, D_0 \equiv 1 \pmod 8$ or $m_1 \equiv 7 \pmod 8, D_0 \equiv 5 \pmod 8$, then $(-1)^{\frac{\frac{D_0 m^2 m_1 - 1}{2} - 1}{2}} = (-1)^{\frac{\frac{8\ell+3-1}{2}-1}{2}} = (-1)^{2\ell} = 1$. Either case, we have

$$N_{D,d}(2^{2e+1}) = (-1)^k \left(\frac{D_0}{2}\right) 2^e.$$

□

Proof of Claim IV. Since the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^n}$ for $n \equiv 2e+2$ has no solution as in Case 2(ii)(b), $N_{D,d}(2^n) = 0$ for $n \equiv 2e+2$. □

2.4.12 Case 2(iv)(a)

Proof of Proposition 2.8 in **Case 2(iv)(a)**. Recall the assumptions: $p|f$, $p|d$ and $p|D_0$ with p odd.

We also compute $N_{D,d}(p^n)$ here. We make the following claims in this part of the sub-case:

I. $N_{D,d}(p^{2n+1}) = 0$ for $0 \leq n \leq e-1$.

II. $N_{D,d}(p^{2n}) = (-1)^k(p^n - p^{n-1})$ for $1 \leq n \leq e$.

III. $N_{D,d}(p^{2e+1}) = 0$.

IV. $N_{D,d}(p^{2e+2}) = (-1)^{k+1}p^e$.

V. $N_{D,d}(p^n) = 0$ for $n \geq 2e+3$.

Then, we have

$$\begin{aligned}
L.H.S. =& 1 + \frac{p-1}{p^{2k}} + \frac{p^2-p}{p^{4k}} + \frac{p^3-p^2}{p^{6k}} + \cdots + \frac{p^e - p^{e-1}}{p^{2ek}} - \frac{p^e}{p^{(2e+2)k}} \\
=& 1 + \frac{1}{p^{2k-1}} + \frac{1}{p^{2(2k-1)}} + \cdots + \frac{1}{p^{e(2k-1)}} \\
& - \left(\frac{1}{p^{2k}} + \frac{1}{p^{4k-1}} + \frac{1}{p^{6k-2}} + \cdots + \frac{1}{p^{2ek-e+1}} + \frac{1}{p^{2ek+2k-e}}\right) \\
=& \frac{\sigma_{2k-1}(p^e)}{p^{e(2k-1)}} - \left(\frac{1}{p^{2k}} + \frac{1}{p^{2k-1+2k}} + \frac{1}{p^{2(2k-1)+2k}} + \cdots + \frac{1}{p^{(e-1)(2k-1)+2k}} + \frac{1}{p^{e(2k-1)+2k}}\right) \\
=& \frac{\sigma_{2k-1}(p^e)}{p^{e(2k-1)}} - \frac{1}{p^{2k}} \frac{\sigma_{2k-1}(p^e)}{p^{e(2k-1)}} \\
=& (1 - p^{-2k}) \frac{1}{p^{e(2k-1)}} \sigma_{2k-1}(p^e) \\
=& R.H.S.
\end{aligned}$$

□

Proof of Claim I and II. In this case, everything follows as same as Case 2(iii)(a) up to the point that the equation $b^2 - Dd \equiv 0 \pmod{p^{2e+1}}$ has the solution set $\{t_{e+1}p^{e+1} + t_{e+2}p^{e+2} + \cdots + t_{2e}p^{2e}\}$ with $t_i \in \{0, 1, ..., p-1\}$. Thus, $N_{D,d}(p^{2n+1}) = 0$ for all $0 \le n \le e-1$ and $N_{D,d}(p^{2n}) = (-1)^k p^n - p^{n-1}$ for all $0 \le n \le e$. □

Proof of Claim III. Recall that the equation $b^2 - Dd \equiv 0 \pmod{p^{2e+1}}$ has the solution set $\{t_{e+1}p^{e+1} + \cdots + t_{2e-1}p^{2e-1} + t_{2e}p^{2e}\}$ with $t_i \in \{0, 1, ..., p-1\}$. Then, the equation $b^2 - Dd \equiv 0 \pmod{4p^{2e+1}}$ with $0 \le b \le 2p^{2e+1}$ also has p^e solutions, $b_t = t_{e+1}p^{e+1} + \cdots + t_{2e-1}p^{2e-1} + t_{2e}p^{2e} + m_t p^{2e+1}$ for some fixed integer m_t. Let $c_t = \frac{Dd - b_t^2}{4p^{2e+1}}$. Then

$$
\begin{aligned}
N_{D,d}(p^{2e+1}) &= \sum_{t=1}^{p^e} \chi_d([-p^{2e+1}, b_t, c_t]) \\
&= \begin{cases} \sum_{t=1}^{p^e} \left(\frac{\frac{d}{p}}{-p^{2e+1}}\right)\left(\frac{p}{c_t}\right) & \text{if } p \equiv 1 \pmod 4, \\ \sum_{t=1}^{p^e} \left(\frac{-\frac{d}{p}}{-p^{2e+1}}\right)\left(\frac{-p}{c_t}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases} \\
&= \begin{cases} \left(\frac{\frac{d}{p}}{-p}\right) \sum_{t=1}^{p^e} \left(\frac{c_t}{p}\right) & \text{if } p \equiv 1 \pmod 4, \\ \left(\frac{-\frac{d}{p}}{-p}\right) \sum_{t=1}^{p^e} \left(\frac{c_t}{p}\right) & \text{if } p \equiv 3 \pmod 4. \end{cases}
\end{aligned}
$$

However,

$$
\begin{aligned}
c_t &= \frac{Dd - (t_{e+1}p^{e+1} + t_{e+2}p^{e+2} + \cdots + t_{2e}p^{2e} + m_t p^{2e+1})^2}{4p^{2e+1}} \\
&= \frac{D_0 p^{2e} m^2 d - (t_{e+1} + t_{e+2}p + \cdots + t_{2e}p^{e-1} + m_t p^e)^2 p^{2e+2}}{4p^{2e+1}} \\
&= \frac{\frac{D_0}{p} m^2 d - (t_{e+1} + t_{e+2}p + \cdots + t_{2e}p^{e-1} + m_t p^e)^2 p}{4},
\end{aligned}
$$

and $p | c_t$. Thus, $N_{D,d}(p^{2e+1}) = 0$. □

Proof of Claim IV. For the equation $b^2 - Dd \equiv 0 \pmod{p^{2e+2}}$, we see that

$$
\begin{aligned}
&(t_{e+1}p^{e+1} + t_{e+2}p^{e+2} + \cdots + t_{2e-1}p^{2e-1} + t_{2e}p^{2e})^2 - Dd \equiv 0 \pmod{p^{2e+2}} \\
\Longleftrightarrow &(t_{e+1} + t_{e+2}p + \cdots + t_{2e}p^{e-1})^2 p^{2e+2} - D_0 p^{2e} m^2 d \equiv 0 \pmod{p^{2e+2}} \\
\Longleftrightarrow &0 \equiv 0 \pmod{p^{2e+2}},
\end{aligned}
$$

which is always true. Thus, the equation $b^2 - Dd \equiv 0 \pmod{p^{2e+2}}$ has the solution set $\{t_{e+1}p^{e+1} + t_{e+2}p^{e+2} + \cdots + t_{2e}p^{2e} + t_{2e+1}p^{2e+1}\}$ with $t_i \in \{0, 1, ..., p-1\}$. Then, the equation $b^2 - Dd \equiv$

$0 \pmod{4p^{2e+2}}$ with $0 \le b \le 2p^{2e+1}$ also has p^{e+1} solutions, $b_t = t_{e+1}p^{e+1} + \cdots + t_{2e-1}p^{2e-1} + t_{2e}p^{2e} + t_{2e+1}p^{2e+1} + m_t p^{2e+2}$ for some fixed integer m_t. Let $c_t = \frac{Dd - b_t^2}{4p^{2e+2}}$. Now,

$$\begin{aligned} N_{D,d}(p^{2e+2}) &= \sum_{t=1}^{p^{e+1}} \chi_d([-p^{2e+2}, b_t, c_t]) \\ &= \begin{cases} \sum_{t=1}^{p^{e+1}} \left(\frac{\frac{d}{p}}{-p^{2e+2}}\right)\left(\frac{p}{c_t}\right) & \text{if } p \equiv 1 \pmod 4, \\ \sum_{t=1}^{p^{e+1}} \left(\frac{-\frac{d}{p}}{-p^{2e+2}}\right)\left(\frac{-p}{c_t}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases} \\ &= \begin{cases} (-1)^k \sum_{t=1}^{p^{e+1}} \left(\frac{c_t}{p}\right) & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{k+1} \sum_{t=1}^{p^{e+1}} \left(\frac{c_t}{p}\right) & \text{if } p \equiv 3 \pmod 4. \end{cases} \end{aligned}$$

Then, we have

$$\begin{aligned} &\sum_{t=1}^{p^{e+1}} \left(\frac{c_t}{p}\right) \\ &= \sum_{t_{e+1}=0}^{p-1} \sum_{t_{e+2}=0}^{p-1} \cdots \sum_{t_{2e+1}=0}^{p-1} \left(\frac{\frac{Dd-(t_{e+1}p^{e+1}+t_{e+2}p^{e+2}+\cdots+t_{2e+1}p^{2e+1}+m_t p^{2e+2})^2}{4p^{2e+2}}}{p}\right) \\ &= \sum_{t_{e+1}=0}^{p-1} \sum_{t_{e+2}=0}^{p-1} \cdots \sum_{t_{2e+1}=0}^{p-1} \left(\frac{\frac{D_0 p^{2e} m^2 d-(t_{e+1}+t_{e+2}p+\cdots+t_{2e+1}p^{e}+m_t p^{e+1})^2 p^{2e+2}}{p^{2e+2}}}{p}\right) \\ &= \sum_{t_{e+1}=0}^{p-1} \sum_{t_{e+2}=0}^{p-1} \cdots \sum_{t_{2e+1}=0}^{p-1} \left(\frac{\frac{D_0}{p} m^2 \frac{d}{p} - (t_{e+1}+t_{e+2}p+\cdots+t_{2e+1}p^{e}+m_t p^{e+1})^2}{p}\right) \\ &= \sum_{t_{e+1}=0}^{p-1} \sum_{t_{e+2}=0}^{p-1} \cdots \sum_{t_{2e+1}=0}^{p-1} \left(\frac{\frac{D_0}{p} m^2 \frac{d}{p} - t_{e+1}^2}{p}\right) \\ &= \left(\frac{-1}{p}\right) \sum_{t_{e+1}=0}^{p-1} \sum_{t_{e+2}=0}^{p-1} \cdots \sum_{t_{2e+1}=0}^{p-1} \left(\frac{t_{e+1}^2 - \frac{D_0}{p} m^2 \frac{d}{p}}{p}\right) \\ &= \left(\frac{-1}{p}\right) \sum_{t_{e+1}=0}^{p-1} \sum_{t_{e+2}=0}^{p-1} \cdots \sum_{t_{2e+1}=0}^{p-1} (-1) \\ &= \left(\frac{-1}{p}\right)(-p^e). \end{aligned}$$

Thus, $N_{D,d}(p^{2e+2}) = (-1)^k(-p^e) = (-1)^{k+1}p^e$. □

Proof of Claim V. For the equation $b^2 - Dd \equiv 0 \pmod{p^{2e+3}}$, we see that

$$\begin{aligned}
&(t_{e+1}p^{e+1} + t_{e+2}p^{e+2} + \cdots + t_{2e+1}p^{2e+1})^2 - Dd \equiv 0 \pmod{p^{2e+3}}\\
\Longleftrightarrow&(t_{e+1} + t_{e+2}p + \cdots + t_{2e+1}p^{e})^2 p^{2e+2} - D_0 p^{2e} m^2 d \equiv 0 \pmod{p^{2e+3}}\\
\Longleftrightarrow&(t_{e+1} + t_{e+2}p + \cdots + t_{2e+1}p^{e})^2 - \frac{D_0}{p} m^2 \frac{d}{p} \equiv 0 \pmod{p}\\
\Longleftrightarrow&t_{e+1}^2 - \frac{D_0}{p} m^2 \frac{d}{p} \equiv 0 \pmod{p}\\
\Longleftrightarrow&\left(\frac{\frac{D_0}{p}\frac{d}{p}}{p}\right) = 1.
\end{aligned}$$

Thus, if $\left(\frac{\frac{D_0}{p}\frac{d}{p}}{p}\right) = -1$, no solution is lifted and $N_{D,d}(p^n) = 0$ for all $n \geq 2e+3$. If $\left(\frac{\frac{D_0}{p}\frac{d}{p}}{p}\right) = 1$, then the solutions $\pm(t_{e+1}p^{e+1} + t_{e+2}p^{e+2} + \cdots + t_{2e+1}p^{2e+1})$ (with specific $t_{e+1} \neq 0$) is lifted. Thus, the equation $b^2 - Dd \equiv 0 \pmod{p^{2e+3}}$ has the solution set $\{\pm(t_{e+1}p^{e+1} + t_{e+2}p^{e+2} + \cdots + t_{2e+1}p^{2e+1} + t_{2e+2}p^{2e+2})\}$ with $t_{e+2}, t_{e+3}..., t_{2e+2} \in \{0, 1, ..., p-1\}$ and there are $2p^{e+1}$ solutions.

For the equation $b^2 - Dd \equiv 0 \pmod{p^{2e+4}}$, consider

$$\begin{aligned}
&(t_{e+1}p^{e+1} + t_{e+2}p^{e+2} + \cdots + t_{2e+2}p^{2e+2})^2 - Dd \equiv 0 \pmod{p^{2e+4}}\\
\Longleftrightarrow&(t_{e+1} + t_{e+2}p + \cdots + t_{2e+2}p^{e+1})^2 p^{2e+2} - D_0 p^{2e} m^2 d \equiv 0 \pmod{p^{2e+4}}\\
\Longleftrightarrow&(t_{e+1} + t_{e+2}p + \cdots + t_{2e+1}p^{e})^2 - \frac{D_0}{p} m^2 \frac{d}{p} \equiv 0 \pmod{p^2}\\
\Longleftrightarrow&(t_{e+1} + t_{e+2}p)^2 - \frac{D_0}{p} m^2 \frac{d}{p} \equiv 0 \pmod{p^2}\\
\Longleftrightarrow&t_{e+1}^2 + 2t_{e+1}t_{e+2}p - \frac{D_0}{p} m^2 \frac{d}{p} \equiv 0 \pmod{p^2}\\
\Longleftrightarrow&\frac{t_{e+1}^2 - \frac{D_0}{p} m^2 \frac{d}{p}}{p} + 2t_{e+1}t_{e+2} \equiv 0 \pmod{p}.
\end{aligned}$$

Thus, we have a linear equation here and there is a specific solution t_{e+2} that works. Thus, the equation $b^2 - Dd \equiv 0 \pmod{p^{2e+4}}$ has the solution set $\{\pm(t_{e+1}p^{e+1} + t_{e+2}p^{e+2} + \cdots + t_{2e+2}p^{2e+2} + t_{2e+3}p^{2e+3})\}$ with $t_{e+3}, t_{e+4}..., t_{2e+3} \in \{0, 1, ..., p-1\}$, and there are $2p^{e+1}$ solutions. Similar to before, the equation $b^2 - Dd \equiv 0 \pmod{p^{2e+s}}$ for $s \geq 3$ always has $2p^{e+1}$ solutions with the solution set $\{\pm(t_{e+1}p^{e+1} + t_{e+2}p^{e+2} + \cdots + t_{2e+s-1}p^{2e+s-1})\}$ with $t_{e+s-1}, t_{e+s}..., t_{2e+s-1} \in \{0, 1, ..., p-1\}$.

Then, the equation $b^2 - Dd \equiv 0 \pmod{4p^{2e+s}}$ with $0 \leq b \leq 2p^{2e+1}$ has $2p^{e+1}$ solutions, $b_t = \pm(t_{e+1}p^{e+1} + t_{e+2}p^{e+2} + \cdots + t_{2e+s-1}p^{2e+s-1} + m_t p^{2e+s})$ for some fixed integer m_t. Let $c_t = \frac{Dd - b_t^2}{4p^{2e+s}}$.

Now,

$$N_{D,d}(p^{2e+s}) = \sum_{t=1}^{2p^{e+1}} \chi_d([-p^{2e+s}, b_t, c_t])$$
$$= \begin{cases} \sum_{t=1}^{2p^{e+1}} \left(\frac{\frac{d}{p}}{-p^{2e+s}}\right)\left(\frac{p}{c_t}\right) & \text{if } p \equiv 1 \pmod 4, \\ \sum_{t=1}^{2p^{e+1}} \left(\frac{-\frac{d}{p}}{-p^{2e+s}}\right)\left(\frac{-p}{c_t}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases}$$
$$= \begin{cases} \left(\frac{\frac{d}{p}}{-p^{s}}\right) \sum_{t=1}^{2p^{e+1}} \left(\frac{c_t}{p}\right) & \text{if } p \equiv 1 \pmod 4, \\ \left(\frac{-\frac{d}{p}}{-p^{s}}\right) \sum_{t=1}^{2p^{e+1}} \left(\frac{c_t}{p}\right) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Now, we have

$$\sum_{t=1}^{2p^{e+1}} \left(\frac{c_t}{p}\right)$$
$$= \sum_{t_{e+s-1}=0}^{p-1} \sum_{t_{e+s}=0}^{p-1} \cdots \sum_{t_{2e+s-1}=0}^{p-1} \left(\frac{\frac{Dd-(t_{e+1}p^{e+1}+t_{e+2}p^{e+2}+\cdots+t_{2e+s-1}p^{2e+s-1}+m_t p^{2e+s})^2}{4p^{2e+s}}}{p}\right)$$
$$= \sum_{t_{e+s-1}=0}^{p-1} \sum_{t_{e+s}=0}^{p-1} \cdots \sum_{t_{2e+s-1}=0}^{p-1} \left(\frac{\frac{Dd-(t_{e+1}p^{e+1}+t_{e+2}p^{e+2}+\cdots+t_{2e+s-1}p^{2e+s-1})^2}{p^{2e+s}}}{p}\right)$$
$$= \sum_{t_{e+s-1}=0}^{p-1} \sum_{t_{e+s}=0}^{p-1} \cdots \sum_{t_{2e+s-1}=0}^{p-1} \left(\frac{\frac{\frac{D_0}{p}m^2\frac{d}{p}-(t_{e+1}+t_{e+2}p+\cdots+t_{2e+s-1}p^{e+s-2})^2}{p^{s-2}}}{p}\right)$$
$$= \sum_{t_{e+s-1}=0}^{p-1} \sum_{t_{e+s}=0}^{p-1} \cdots \sum_{t_{2e+s-1}=0}^{p-1} \left(\frac{\frac{\frac{D_0}{p}m^2\frac{d}{p}-(t_{e+1}+t_{e+2}p+\cdots+t_{2e+s-2}p^{e+s-3})^2}{p^{s-2}} + 2t_{e+1}t_{e+s-1}}{p}\right)$$
$=0$ (since the top is always a linear equation in t_{e+s-1}).

Thus, $N_{D,d}(p^{2e+s}) = 0$ for all $s \geq 3$. □

2.4.13 Case 2(iv)(b)

Proof of Proposition 2.8 in **Case 2(iv)(b)**. Recall the assumptions: $p|f$, $p|d$ and $p|D_0$ with $p = 2$.

In this part of the sub-case, we make the same claims as the previous part:

I. $N_{D,d}(2^{2n+1}) = 0$ for $0 \leq n \leq e-1$.

II. $N_{D,d}(2^{2n}) = (-1)^k(2^s - 2^{s-1})$ for $1 \leq n \leq e$.

III. $N_{D,d}(2^{2e+1}) = 0$.

IV. $N_{D,d}(2^{2e+2}) = (-1)^{k+1}2^e$.

V. $N_{D,d}(2^n) = 0$ for $n \geq 2e+3$.

Thus, the rest is exactly the same as the previous part of the sub-case. □

Proof of Claim I and II. Write $d = 4m_1$ and $D_0 = 4m_2$. Then $Dd = 2^{2e+4}m_1m_2m^2$. The solution sets stay the same as in Case 2(iii)(b) up to the point that the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e}}$ has the solution set $\{2^{e+1}t\}_{t=0}^{t=2^{e+1}-1}$. Thus, everything in Claim I and Claim II follows as in Case 2(iii)(b) except that in the calculation of $N_{D,d}(2^{2e})$, we have c_t is even if t is even. Then it follows from calculating $N_{D,d}(2^{2n})$ for $n \leq e$. □

Proof of Claim III, IV and V. For this and the rest claims, we will consider three cases: $m_1 \equiv m_2 \equiv 3 \pmod 4$, m_1 or $m_2 \equiv 2 \pmod 4$ and $m_1 \equiv m_2 \equiv 2 \pmod 4$.

First consider the case $m_1 \equiv m_2 \equiv 3 \pmod 4$. We use the same technique to determine the solution sets for the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+n}}$ for $n \geq 1$.

For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+1}}$, all the previous solutions are lifted to the solution set $\{2^{e+2}t\}_{t=0}^{t=2^{e+1}-1}$.

For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+2}}$, all the previous solutions are lifted to the solution set $\{2^{e+2}t\}_{t=0}^{t=2^{e+2}-1}$.

For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+3}}$, half of the previous solutions are lifted to the solution set $\{2^{e+2}(2t+1)\}_{t=0}^{t=2^{e+2}-1}$.

For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+4}}$, all of the previous solutions are lifted to the solution set $\{2^{e+2}(2t+1)\}_{t=0}^{t=2^{e+3}-1} = \{\pm 2^{e+2}(4t+1)\}_{t=0}^{t=2^{e+2}-1}$.

For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+5}}$, if $m_1m_2m^2 \equiv 1 \pmod 8$, all of the previous solutions are lifted to the solution set $\{\pm 2^{e+2}(4t+1)\}_{t=0}^{t=2^{e+3}-1}$, otherwise there is no solution.

For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+5+n}}$, $n \geq 1$, if $m_1m_2m^2 \equiv 2^3r + 1 \pmod{2^{n+3}}$ for some $r \in \{0, 1, ..., 2^n - 1\}$, half of the previous solutions are lifted to the solution set $\{\pm 2^{e+2}(2^{n+2}t + 2^2s + 1)\}_{t=0}^{t=2^{e+3}-1}$ for some $s \in \{0, 1, ..., 2^n - 1\}$ such that $(2^2s+1)^2 \equiv 2^3r + 1 \pmod{2^n + 3}$.

To find $N_{D,d}(2^{2e+1})$, we note that the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+1}}$ has the solution set $\{2^{e+2}t\}_{t=0}^{t=2^{e+1}-1}$. Let $c_t = \frac{Dd - b_t^2}{4 \cdot 2^{2e+1}} = \frac{2^{2e+4}m_1m_2m^2 - 2^{2e+4}t^2}{2^{2e+3}} = 2m_1m_2m^2 - 2t^2$. Since $2|c_t$, we have

$$N_{D,d}(2^{2e+1}) = \sum_{t=0}^{2^e-1} \chi_d([-2^{2e+1}, 2^{e+2}t, c_t]) = 0.$$

To find $N_{D,d}(2^{2e+2})$, we note that the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+2}}$ has the solution set $\{2^{e+2}t\}_{t=0}^{t=2^{e+2}-1}$. Let $c_t = \frac{Dd-(2^{e+2}t)^2}{4\cdot 2^{2e+2}} = \frac{2^{2e+4}m_1m_2m^2-2^{2e+4}t^2}{2^{2e+4}} = m_1m_2m^2 - t^2$. Then,

$$\begin{aligned}
N_{D,d}(2^{2e+2}) &= \sum_{t=0}^{2^{e+1}-1} \chi_d([-2^{2e+2}, 2^{e+2}t, c_t]) \\
&= \sum_{t=0}^{2^{e+1}-1} \left(\frac{-m_1}{-2^{2e+2}}\right)\left(\frac{-4}{c_t}\right) \\
&= \left(\frac{-m_1}{-1}\right) \sum_{t=0,2,\ldots,2^{e+1}-2} \left(\frac{-1}{c_t}\right) \\
&= (-1)^{k+1} \sum_{t=0,2,\ldots,2^{e+1}-2} (-1)^{\frac{c_t-1}{2}} \\
&= (-1)^{k+1} \sum_{t=0,2,\ldots,2^{e+1}-2} (-1)^{\frac{m_1m_2m^2-t^2-1}{2}} \\
&= (-1)^{k+1} \sum_{t=0,2,\ldots,2^{e+1}-2} 1 \\
&= (-1)^{k+1}2^e \\
&= (-1)^k(-2^e).
\end{aligned}$$

To find $N_{D,d}(2^{2e+3})$, we note that the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+3}}$ has the solution set $\{2^{e+2}(2t+1)\}_{t=0}^{t=2^{e+2}-1}$. Let $c_t = \dfrac{Dd-(2^{e+2}(2t+1)^2}{4\cdot 2^{2e+3}} = \dfrac{2^{2e+4}m_1m_2m^2 - 2^{2e+4}(2t+1)^2}{2^{2e+5}} = \dfrac{m_1m_2m^2-(2t+1)^2}{2} = \dfrac{m_1m_2m^2-1}{2} - 2t^2 - 2t$. We know that $\frac{m_1m_2m^2-1}{2}$ is divisible by 2 because $m_1m_2m^2 \equiv 1 \pmod 4$. Thus, $2|c_t$. Then,

$$N_{D,d}(2^{2e+3}) = \sum_{t=0}^{2^{e+1}-1} \chi_d([-2^{2e+3}, 2^{e+2}(2t+1), c_t]) = 0.$$

To find $N_{D,d}(2^{2e+4})$, we note that the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+4}}$ has the solution set $\{\pm 2^{e+2}(4t+1)\}_{t=0}^{t=2^{e+2}-1}$. Let $b_t = 2^{e+2}(4t+1)$ and $c_t = \dfrac{Dd-(2^{e+2}(4t+1)^2}{4\cdot 2^{2e+4}} = \dfrac{2^{2e+4}m_1m_2m^2-2^{2e+4}(4t+1)^2}{2^{2e+6}} = \dfrac{m_1m_2m^2-(4t+1)^2}{4} = \dfrac{m_1m_2m^2-1}{4} - 4t^2 - 2t = c_0 - 4t^2 - 2t$. If c_0 is even, then so is c_t and $N_{D,d}(2^{2e+4}) = 0$. So we can assume c_0 is odd. Then,

$$
\begin{aligned}
N_{D,d}(2^{2e+4}) &= \sum_{t=0}^{2^{e+2}-1} \chi_d([-2^{2e+4}, 2^{e+2}(4t+1), c_t]) \\
&= \sum_{t=0}^{2^{e+2}-1} \left(\frac{-m_1}{-2^{2e+4}}\right)\left(\frac{-4}{c_t}\right) \\
&= (-1)^{k+1} \sum_{t=0}^{2^{e+2}-1} \left(\frac{-1}{c_t}\right) \\
&= (-1)^{k+1} \sum_{t=0}^{2^{e+2}-1} (-1)^{\frac{c_t-1}{2}} \\
&= (-1)^{k+1} \sum_{t=0}^{2^{e+2}-1} (-1)^{\frac{c_0-4t^2-2t-1}{2}} \\
&= (-1)^{k+1} \sum_{t=0}^{2^{e+2}-1} (-1)^{\frac{c_0-1}{2}-2t^2-t} \\
&= (-1)^{k+1}(-1)^{\frac{c_0-1}{2}} \sum_{t=0}^{2^{e+2}-1} (-1)^{-t} \\
&= 0.
\end{aligned}
$$

To find $N_{D,d}(2^{2e+5})$, we note that the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+5}}$ has the solution set $\{\pm 2^{e+2}(4t+1)\}_{t=0}^{t=2^{e+3}-1}$ if $m_1m_2m^2 \equiv 1 \pmod 8$. Otherwise, there is no solution and $N_{D,d}(2^{2e+4}) = 0$. Thus, assume $m_1m_2m^2 \equiv 1 \pmod 8$. Indeed, we can consider $N_{D,d}(2^{2e+5+n})$ for $n \geq 0$ all at once.

For $n \geq 1$, if $m_1m_2m^2 \equiv 2^3r + 1 \pmod{2^{n+3}}$ for some $r \in \{0, 1, ..., 2^n - 1\}$, the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+5+n}}$ has the solution set $\{\pm 2^{e+2}(2^{n+2}t + 2^2s + 1)\}_{t=0}^{t=2^{e+3}-1}$ for some $s \in \{0, 1, ..., 2^n - 1\}$ such that $(2^2s + 1)^2 \equiv 2^3r + 1 \pmod{2^n + 3}$. For $n = 0$, we take $r = s = 0$. Then, let $b_t = 2^{e+2}(2^{n+2}t + 2^2s + 1)$ and

$$
\begin{aligned}
c_t &= \frac{2^{2e+4}m_1m_2m^2 - 2^{2e+4}(2^{n+2}t + 2^2s + 1)^2}{4 \cdot 2^{2e+5+n}} \\
&= \frac{m_1m_2m^2 - (2^{n+2}t + 2^2s + 1)^2}{2^{n+3}} \\
&= \frac{m_1m_2m^2 - 2^{2n+4}t^2 - 2^{n+3}t(4s+1) - (4s+1)^2}{2^{n+3}} \\
&= \frac{m_1m_2m^2 - (4s+1)^2}{2^{n+3}} - 2^{n+1}t^2 - (4s+1)t \\
&= c_0 - 2^{n+1}t^2 - (4s+1)t.
\end{aligned}
$$

Then, we have

$$\begin{aligned}N_{D,d}(2^{2e+5+n}) &= \sum_{t=0}^{2^{e+3}-1} \chi_d([-2^{2e+5+n}, b_t, c_t]) \\ &= \sum_{t=0}^{2^{e+3}-1} \left(\frac{-m_1}{-2^{2e+5+n}}\right)\left(\frac{-4}{c_t}\right) \\ &= \left(\frac{-m_1}{-2^{n+1}}\right) \sum_{t=0}^{2^{e+3}-1} \left(\frac{-4}{c_t}\right).\end{aligned}$$

Consider

$$\sum_{t=0}^{2^{e+3}-1} \left(\frac{-4}{c_t}\right) = \begin{cases} \sum_{t \text{ odd}} \left(\frac{-4}{c_t}\right) & \text{if } c_0 \text{ is even,} \\ \sum_{t \text{ even}} \left(\frac{-4}{c_t}\right) & \text{if } c_0 \text{ is odd} \end{cases}.$$

We see that

$$\begin{aligned}\sum_{t \text{ odd or even}} \left(\frac{-4}{c_t}\right) &= \sum_{t \text{ odd or even}} \left(\frac{-1}{c_t}\right) \\ &= \sum_{t \text{ odd or even}} (-1)^{\frac{c_t-1}{2}} \\ &= \sum_{t \text{ odd or even}} (-1)^{\frac{c_0-2^{n+1}t^2-(4s+1)t-1}{2}} \\ &= \sum_{t \text{ odd or even}} (-1)^{\frac{c_0-t-1}{2}-2^n t^2-2st} \\ &= \sum_{t \text{ odd or even}} (-1)^{\frac{c_0-t-1}{2}-2^n t^2} \\ &= 0.\end{aligned}$$

Thus, $N_{D,d}(2^{2e+5+n}) = 0$ for all $n \geq 0$.

Now consider the case m_1 or $m_2 \equiv 2 \pmod 4$.

For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+1}}$, the solution set is $\{2^{e+2}t\}_{t=0}^{t=2^{e+1}-1}$.
For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+2}}$, the solution set is $\{2^{e+2}t\}_{t=0}^{t=2^{e+2}-1}$.
For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+3}}$, the solution set is $\{2^{e+3}t\}_{t=0}^{t=2^{e+2}-1}$.
For the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+4}}$, there is no solution.

To find $N_{D,d}(2^{2e+1})$, we note that the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+1}}$ has the solution set $\{2^{e+2}t\}_{t=0}^{t=2^{e+1}-1}$. Let $c_t = \frac{Dd-b_t^2}{4 \cdot 2^{2e+1}} = \frac{2^{2e+4}m_1m_2m^2 - 2^{2e+4}t^2}{2^{2e+3}} = 2m_1m_2m^2 - 2t^2$. Since $2|c_t$, we have

$$N_{D,d}(2^{2e+1}) = \sum_{t=0}^{2^e-1} \chi_d([-2^{2e+1}, 2^{e+2}t, c_t]) = 0.$$

To find $N_{D,d}(2^{2e+2})$, we note that the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+2}}$ has the solution set $\{2^{e+2}t\}_{t=0}^{t=2^{e+2}-1}$. Let $c_t = \frac{Dd-(2^{e+2}t)^2}{4 \cdot 2^{2e+2}} = \frac{2^{2e+4}m_1m_2m^2-2^{2e+4}t^2}{2^{2e+4}} = m_1m_2m^2 - t^2 = c_0 - t^2$. Then,

$$\begin{aligned}
N_{D,d}(2^{2e+2}) &= \sum_{t=0}^{2^{e+1}-1} \chi_d([-2^{2e+2}, 2^{e+2}t, c_t]) \\
&= \begin{cases} \sum_{t=0}^{2^{e+1}-1} \left(\frac{-m_1}{-2^{2e+2}}\right)\left(\frac{-4}{c_t}\right) & \text{if } m_1 \equiv 3 \pmod 4, \\ \sum_{t=0}^{2^{e+1}-1} \left(\frac{\frac{m_1}{2}}{-2^{2e+2}}\right)\left(\frac{8}{c_t}\right) & \text{if } m_1 \equiv 2 \pmod 8, \\ \sum_{t=0}^{2^{e+1}-1} \left(\frac{-\frac{m_1}{2}}{-2^{2e+2}}\right)\left(\frac{-8}{c_t}\right) & \text{if } m_1 \equiv 6 \pmod 8 \end{cases} \\
&= \begin{cases} (-1)^{k+1} \sum_{t=0}^{2^{e+1}-1} \left(\frac{-4}{c_t}\right) & \text{if } m_1 \equiv 3 \pmod 4, \\ (-1)^{k} \sum_{t=0}^{2^{e+1}-1} \left(\frac{2}{c_t}\right) & \text{if } m_1 \equiv 2 \pmod 8, \\ (-1)^{k+1} \sum_{t=0}^{2^{e+1}-1} \left(\frac{-2}{c_t}\right) & \text{if } m_1 \equiv 6 \pmod 8. \end{cases}
\end{aligned}$$

If $m_1 \equiv 3 \pmod 4$, we have

$$\begin{aligned}
N_{D,d}(2^{2e+2}) &= (-1)^{k+1} \sum_{t=0}^{2^{e+1}-1} \left(\frac{-4}{c_t}\right) \\
&= (-1)^{k+1} \sum_{t=1,3,\ldots,2^{e+1}-1} \left(\frac{-1}{c_t}\right) \\
&= (-1)^{k+1} \sum_{t=1,3,\ldots,2^{e+1}-1} (-1)^{\frac{c_t-1}{2}} \\
&= (-1)^{k+1} \sum_{t=1,3,\ldots,2^{e+1}-1} (-1)^{\frac{m1m2m^2-t^2-1}{2}} \\
&= (-1)^{k+1}(-1)^{\frac{m1m2m^2}{2}} \sum_{t=1,3,\ldots,2^{e+1}-1} (-1)^{\frac{-t^2-1}{2}} \\
&= (-1)^{k} \sum_{t=1,3,\ldots,2^{e+1}-1} (-1)^{\frac{t^2+1}{2}} \\
&= (-1)^{k} \sum_{t=1,3,\ldots,2^{e+1}-1} (-1) \\
&= (-1)^k(-2^e) \\
&= (-1)^{k+1}2^e.
\end{aligned}$$

If $m_1 \equiv 2 \pmod 8$, we have

$$\begin{aligned}
N_{D,d}(2^{2e+2}) &= (-1)^k \sum_{t=0}^{2^{e+1}-1} \left(\frac{2}{c_t}\right) \\
&= (-1)^k \sum_{t=0}^{2^{e+1}-1} \left(\frac{c_t}{2}\right) \\
&= (-1)^k \sum_{t=1,3,\ldots,2^{e+1}-1} \left(\frac{c_t}{2}\right) \\
&= (-1)^k \sum_{t=1,3,\ldots,2^{e+1}-1} \left(\frac{m_1 m_2 m^2 - t^2}{2}\right) \\
&= (-1)^k \left(\frac{m_1 m_2 - 1}{2}\right) (2^e) \\
&= (-1)^k (-1)(2^e) \\
&= (-1)^{k+1} 2^e.
\end{aligned}$$

If $m_1 \equiv 6 \pmod 8$, we have

$$\begin{aligned}
N_{D,d}(2^{2e+2}) &= (-1)^{k+1} \sum_{t=0}^{2^{e+1}-1} \left(\frac{-2}{c_t}\right) \\
&= (-1)^{k+1} \sum_{t=1,3,\ldots,2^{e+1}-1} \left(\frac{-2}{c_t}\right) \\
&= (-1)^{k+1} \sum_{t=1,3,\ldots,2^{e+1}-1} \left(\frac{-1}{c_t}\right)\left(\frac{c_t}{2}\right) \\
&= (-1)^{k+1} \sum_{t=1,3,\ldots,2^{e+1}-1} (-1)^{\frac{m_1 m_2 m^2 - t^2 - 1}{2}} \left(\frac{c_t}{2}\right) \\
&= (-1)^{k+1} \sum_{t=1,3,\ldots,2^{e+1}-1} \left(\frac{c_t}{2}\right) \\
&= (-1)^{k+1} 2^e.
\end{aligned}$$

To find $N_{D,d}(2^{2e+3})$, we note that the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+3}}$ has the solution set $\{2^{e+3}t\}_{t=0}^{t=2^{e+2}-1}$. Let $c_t = \dfrac{Dd - b_t^2}{4 \cdot 2^{2e+3}} = \dfrac{2^{2e+4} m_1 m_2 m^2 - 2^{2e+6} t^2}{2^{2e+5}} = \dfrac{m_1 m_2}{2} m^2 - 2t^2 = c_0 - 2t^2$. Then, we have

$$N_{D,d}(2^{2e+3}) = \sum_{t=0}^{2^{e+1}-1} \chi_d([-2^{2e+3}, 2^{e+3}t, c_t])$$

$$= \begin{cases} \sum_{t=0}^{2^{e+1}-1} \left(\frac{-m_1}{-2^{2e+3}}\right)\left(\frac{-4}{c_t}\right) & \text{if } m_1 \equiv 3 \pmod 4, \\ \sum_{t=0}^{2^{e+1}-1} \left(\frac{\frac{m_1}{2}}{-2^{2e+3}}\right)\left(\frac{8}{c_t}\right) & \text{if } m_1 \equiv 2 \pmod 8, \\ \sum_{t=0}^{2^{e+1}-1} \left(\frac{-\frac{m_1}{2}}{-2^{2e+3}}\right)\left(\frac{-8}{c_t}\right) & \text{if } m_1 \equiv 6 \pmod 8) \end{cases}$$

$$= \begin{cases} \left(\frac{-m_1}{-2}\right)\sum_{t=0}^{2^{e+1}-1} \left(\frac{-1}{c_t}\right) & \text{if } m_1 \equiv 3 \pmod 4, \\ \left(\frac{\frac{m_1}{2}}{-2}\right)\sum_{t=0}^{2^{e+1}-1} \left(\frac{2}{c_t}\right) & \text{if } m_1 \equiv 2 \pmod 8, \\ \left(\frac{-\frac{m_1}{2}}{-2}\right)\sum_{t=0}^{2^{e+1}-1} \left(\frac{-2}{c_t}\right) & \text{if } m_1 \equiv 6 \pmod 8. \end{cases}$$

If $m_1 \equiv 3 \pmod 4$, we have

$$\sum_{t=0}^{2^{e+1}-1} \left(\frac{-1}{c_t}\right) = \sum_{t=0}^{2^{e+1}-1} (-1)^{\frac{c_0-2t^2-1}{2}} = \sum_{t=0}^{2^{e+1}-1} (-1)^{\frac{c_0-1}{2}-t^2} = (-1)^{\frac{c_0-1}{2}} \sum_{t=0}^{2^{e+1}-1} (-1)^{t^2} = 0.$$

If $m_1 \equiv 2 \pmod 8$, we have

$$\sum_{t=0}^{2^{e+1}-1} \left(\frac{2}{c_t}\right) = \sum_{t=0}^{2^{e+1}-1} \left(\frac{c_t}{2}\right) = \sum_{t=0}^{2^{e+1}-1} \left(\frac{c_0-2t^2}{2}\right) = 2^e \left[\left(\frac{c_0}{2}\right) + \left(\frac{c_0-2}{2}\right)\right] = 0$$

since $c_0 \equiv 3$ or $7 \pmod 8$.

If $m_1 \equiv 6 \pmod 8$, we have

$$\begin{aligned} \sum_{t=0}^{2^{e+1}-1} \left(\frac{-2}{c_t}\right) &= \sum_{t=0}^{2^{e+1}-1} \left(\frac{-1}{c_t}\right)\left(\frac{c_t}{2}\right) \\ &= \sum_{t=0}^{2^{e+1}-1} (-1)^{\frac{c_0-2t^2-1}{2}} \left(\frac{c_t}{2}\right) \\ &= (-1)^{\frac{c_0-1}{2}} \sum_{t=0}^{2^{e+1}-1} (-1)^{t^2} \left(\frac{c_0-2t^2}{2}\right) \\ &= (-1)^{\frac{c_0-1}{2}} 2^e \left[\left(\frac{c_0}{2}\right) - \left(\frac{c_0-2}{2}\right)\right] \\ &= 0 \end{aligned}$$

since $c_0 \equiv 1$ or $5 \pmod 8$.

We know that $N_{D,d}(2^e+4)=0$ because the equation $b^2-Dd\equiv 0 \pmod{4\cdot 2^{2e+4}}$ has no solution.

We now consider the last case when $m_1\equiv m_2\equiv 2 \pmod 4$.

For the equation $b^2-Dd\equiv 0 \pmod{4\cdot 2^{2e+1}}$, the solution set is $\{2^{e+2}t\}_{t=0}^{t=2^{e+1}-1}$.
For the equation $b^2-Dd\equiv 0 \pmod{4\cdot 2^{2e+2}}$, the solution set is $\{2^{e+2}t\}_{t=0}^{t=2^{e+2}-1}$.
For the equation $b^2-Dd\equiv 0 \pmod{4\cdot 2^{2e+3}}$, the solution set is $\{2^{e+3}t\}_{t=0}^{t=2^{e+2}-1}$.
For the equation $b^2-Dd\equiv 0 \pmod{4\cdot 2^{2e+4}}$, the solution set is $\{2^{e+3}t\}_{t=0}^{t=2^{e+3}-1}$.
For the equation $b^2-Dd\equiv 0 \pmod{4\cdot 2^{2e+5}}$, the solution set is $\{2^{e+3}(2t+1)\}_{t=0}^{t=2^{e+3}-1}$.
For the equation $b^2-Dd\equiv 0 \pmod{4\cdot 2^{2e+6}}$, the solution set is $\{2^{e+3}(2t+1)\}_{t=0}^{t=2^{e+4}-1}=\{\pm 2^{e+3}(4t+1)\}_{t=0}^{t=2^{e+3}-1}$ if $\frac{m_1m_2m^2}{4}\equiv 1 \pmod 4$. Otherwise, there is no solution.
For the equation $b^2-Dd\equiv 0 \pmod{4\cdot 2^{2e+7}}$, the solution set is $\{\pm 2^{e+3}(4t+1)\}_{t=0}^{t=2^{e+4}-1}$ if $\frac{m_1m_2m^2}{4}\equiv 1 \pmod 8$. Otherwise, there is no solution.
For the equation $b^2-Dd\equiv 0 \pmod{4\cdot 2^{2e+7+n}}$, $n\geq 1$, if $\frac{m_1m_2m^2}{4}\equiv 2^3r+1 \pmod{2^{n+3}}$ for some $r\in\{0,1,...,2^n-1\}$, the solution set is $\{\pm 2^{e+3}(2^{n+2}t+2^2s+1)\}_{t=0}^{t=2^{e+4}-1}$ for some $s\in\{0,1,...,2^n-1\}$ such that $(2^2s+1)^2\equiv 2^3r+1 \pmod{2^n+3}$.

To find $N_{D,d}(2^{2e+1})$, it is the same as the previous case.
To find $N_{D,d}(2^{2e+2})$, it is the same as the previous case except there is no $m_1\equiv 3 \pmod 4$.
To find $N_{D,d}(2^{2e+3})$, we note that the equation $b^2-Dd\equiv 0 \pmod{4\cdot 2^{2e+3}}$ has the solution set $\{2^{e+3}t\}_{t=0}^{t=2^{e+2}-1}$. Let $c_t=\frac{Dd-b_t^2}{4\cdot 2^{2e+3}}=\frac{2^{2e+4}m_1m_2m^2-2^{2e+6}t^2}{2^{2e+5}}=\frac{m_1m_2}{2}m^2-2t^2=c_0-2t^2$. However, c_0 is even and $N_{D,d}(2^{2e+3})=0$.
To find $N_{D,d}(2^{2e+4})$, we note that the equation $b^2-Dd\equiv 0 \pmod{4\cdot 2^{2e+4}}$ has the solution set $\{2^{e+3}t\}_{t=0}^{t=2^{e+3}-1}$. Let $c_t=\dfrac{Dd-b_t^2}{4\cdot 2^{2e+4}}=\dfrac{2^{2e+4}m_1m_2m^2-2^{2e+6}t^2}{2^{2e+6}}=\dfrac{m_1m_2m^2}{4}-t^2=c_0-t^2$. Then, we have

$$
\begin{aligned}
N_{D,d}(2^{2e+4}) &= \sum_{t=0}^{2^{e+3}-1} \chi_d([-2^{2e+4}, 2^{e+3}t, c_t]) \\
&= \begin{cases} \sum_{t=0}^{2^{e+3}-1} \left(\frac{-\frac{m_1}{2}}{-2^{2e+4}}\right)\left(\frac{-8}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4, \\ \sum_{t=0}^{2^{e+3}-1} \left(\frac{\frac{m_1}{2}}{-2^{2e+4}}\right)\left(\frac{8}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4 \end{cases} \\
&= \begin{cases} (-1)^{k+1} \sum_{t=0}^{2^{e+3}-1} \left(\frac{-2}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4, \\ (-1)^{k} \sum_{t=0}^{2^{e+3}-1} \left(\frac{2}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4 \end{cases} \\
&= \begin{cases} (-1)^{k+1} \sum_{t=0,2,\ldots,2^{e+3}-2} (-1)^{\frac{c_0-t^2-1}{2}} \left(\frac{c_0-t^2}{2}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4, \\ (-1)^{k} \sum_{t=0,2,\ldots,2^{e+3}-2} \left(\frac{c_0-t^2}{2}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4 \end{cases} \\
&= \begin{cases} (-1)^{k+1}(-1)^{\frac{c_0-1}{2}} \sum_{t=0,2,\ldots,2^{e+3}-2} \left(\frac{c_0-t^2}{2}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4, \\ (-1)^{k} \sum_{t=0,2,\ldots,2^{e+3}-2} \left(\frac{c_0-t^2}{2}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4. \end{cases}
\end{aligned}
$$

However,

$$
\sum_{t=0,2,\ldots,2^{e+3}-2} \left(\frac{c_0-t^2}{2}\right) = (2^{e+2}) \left[\left(\frac{c_0}{2}\right) + \left(\frac{c_0-4}{2}\right)\right] = 0.
$$

Thus, $N_{D,d}(2^{2e+4}) = 0$.

To find $N_{D,d}(2^{2e+5})$, we note that the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+5}}$ has the solution set $\{\pm 2^{e+3}(4t+1)\}_{t=0}^{t=2^{e+2}-1}$. Let $c_t = \dfrac{Dd - b_t^2}{4 \cdot 2^{2e+5}} = \dfrac{2^{2e+4}m_1m_2m^2 - 2^{2e+6}(4t+1)^2}{2^{2e+7}} = \dfrac{m_1m_2m^2-4}{8} - 8t^2 - 4t = c_0 - 8t^2 - 4t$. If c_0 is even, $N_{D,d}(2^{2e+5}) = 0$. Assume c_0 to be odd. Then, we have

$$
\begin{aligned}
N_{D,d}(2^{2e+5}) &= \sum_{t=0}^{2^{e+2}-1} \chi_d([-2^{2e+5}, 2^{e+3}(4t+1), c_t]) \\
&= \begin{cases} \sum_{t=0}^{2^{e+2}-1} \left(\frac{-\frac{m_1}{2}}{-2^{2e+5}}\right)\left(\frac{-8}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4, \\ \sum_{t=0}^{2^{e+2}-1} \left(\frac{\frac{m_1}{2}}{-2^{2e+5}}\right)\left(\frac{8}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4 \end{cases} \\
&= \begin{cases} \left(\frac{-\frac{m_1}{2}}{-2}\right) \sum_{t=0}^{2^{e+2}-1} \left(\frac{-2}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4, \\ \left(\frac{\frac{m_1}{2}}{-2}\right) \sum_{t=0}^{2^{e+2}-1} \left(\frac{2}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4 \end{cases} \\
&= \begin{cases} \left(\frac{-\frac{m_1}{2}}{-2}\right) \sum_{t=0}^{2^{e+2}-1} (-1)^{\frac{c_0-4t-8t^2-1}{2}} \left(\frac{c_t}{2}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4, \\ \left(\frac{\frac{m_1}{2}}{-2}\right) \sum_{t=0}^{2^{e+2}-1} \left(\frac{c_t}{2}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4 \end{cases} \\
&= \begin{cases} \left(\frac{-\frac{m_1}{2}}{-2}\right) (-1)^{\frac{c_0-1}{2}} \sum_{t=0}^{2^{e+2}-1} \left(\frac{c_t}{2}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4, \\ \left(\frac{\frac{m_1}{2}}{-2}\right) \sum_{t=0}^{2^{e+2}-1} \left(\frac{c_t}{2}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4. \end{cases}
\end{aligned}
$$

Now, we have

$$
\begin{aligned}
\sum_{t=0}^{2^{e+2}-1} \left(\frac{c_t}{2}\right) &= \sum_{t=0}^{2^{e+2}-1} \left(\frac{c_0 - 4t - 8t^2}{2}\right) \\
&= \sum_{t=0}^{2^{e+2}-1} \left(\frac{c_0 - 4t}{2}\right) \\
&= 2^{e+1} \left[\left(\frac{c_0}{2}\right) + \left(\frac{c_0 - 4}{2}\right)\right] \\
&= 0.
\end{aligned}
$$

Thus, $N_{D,d}(2^{2e+5}) = 0$.

To find $N_{D,d}(2^{2e+6})$, we note that if $1 - \frac{m_1}{2}\frac{m_2}{2}m^2 \not\equiv 0 \pmod{2^2}$, $N_{D,d}(2^{2e+n}) = 0$ for $n \geq 6$. If $1 - \frac{m_1}{2}\frac{m_2}{2}m^2 \equiv 0 \pmod{2^2}$, the equation $b^2 - Dd \equiv 0 \pmod{4 \cdot 2^{2e+6}}$ has the solution set $\{\pm(2^{e+3}(4t+1)\}_{t=0}^{t=2^{e+3}-1}$. Let $c_t = \dfrac{Dd - (2^{e+3}(4t+1))^2}{2^{2e+8}} = \dfrac{2^{2e+6}\frac{m_1}{2}\frac{m_2}{2}m^2 - 2^{2e+6}(4t+1)^2}{2^{2e+8}} = \dfrac{\frac{m_1}{2}\frac{m_2}{2}m^2 - (4t+1)^2}{4} = \dfrac{\frac{m_1}{2}\frac{m_2}{2}m^2 - 1}{4} - 4t^2 - 2t = c_0 - 4t^2 - 2t$. If c_0 is even, c_t is even and $N_{D,d}(2^{2e+6}) = 0$. Assume c_0 is odd. Then,

$$
\begin{aligned}
N_{D,d}(2^{2e+6}) &= \sum_{t=0}^{2^{e+3}-1} \chi_d([-2^{2e+6}, 2^{e+3}(4t+1), c_t]) \\
&= \begin{cases} \sum_{t=0}^{2^{e+3}-1} \left(\frac{-\frac{m_1}{2}}{-2^{2e+6}}\right)\left(\frac{-8}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4, \\ \sum_{t=0}^{2^{e+3}-1} \left(\frac{\frac{m_1}{2}}{-2^{2e+6}}\right)\left(\frac{8}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4 \end{cases} \\
&= \begin{cases} (-1)^{k+1} \sum_{t=0}^{2^{e+3}-1} (-1)^{\frac{c_t-1}{2}} \left(\frac{c_t}{2}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4, \\ (-1)^{k} \sum_{t=0}^{2^{e+3}-1} \left(\frac{c_t}{2}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4 \end{cases} \\
&= \begin{cases} (-1)^{k+1} \sum_{t=0}^{2^{e+3}-1} (-1)^{\frac{c_0-4t^2-2t-1}{2}} \left(\frac{c_0-2t-4t^2}{2}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4, \\ (-1)^{k} \sum_{t=0}^{2^{e+3}-1} \left(\frac{c_0-4t^2-2t}{2}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4 \end{cases} \\
&= \begin{cases} (-1)^{k+1} \sum_{t=0}^{2^{e+3}-1} (-1)^{\frac{c_0-1}{2}-2t^2-t} \left(\frac{c_0-4t^2-2t}{2}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4, \\ (-1)^{k} \sum_{t=0}^{2^{e+3}-1} \left(\frac{c_0-4t^2-2t}{2}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4 \end{cases} \\
&= \begin{cases} (-1)^{k+1}(-1)^{\frac{c_0-1}{2}} \sum_{t=0}^{2^{e+3}-1} (-1)^{-t} \left(\frac{c_0-2t-4t^2}{2}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4, \\ (-1)^{k} \sum_{t=0}^{2^{e+3}-1} \left(\frac{c_0-2t-4t^2}{2}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4 \end{cases} \\
&= \begin{cases} (-1)^{k+1}(-1)^{\frac{c_0-1}{2}} 2^{e+1} \left[\left(\frac{c_0}{2}\right) - \left(\frac{c_0-6}{2}\right) + \left(\frac{c_0-4}{2}\right) - \left(\frac{c_0-2}{2}\right)\right] & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4, \\ (-1)^{k} 2^{e+1} \left[\left(\frac{c_0}{2}\right) - \left(\frac{c_0-6}{2}\right) + \left(\frac{c_0-4}{2}\right) - \left(\frac{c_0-2}{2}\right)\right] & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4 \end{cases} \\
&= 0.
\end{aligned}
$$

To find $N_{D,d}(2^{2e+7+n})$ for $n \geq 0$, we assume that $\frac{m_1}{2}\frac{m_2}{2}m^2 \equiv 1 \pmod 8$. Otherwise, $N_{D,d}(2^{2e+7+n}) = 0$.

For $n \geq 1$, if $\frac{m_1}{2}\frac{m_2}{2}m^2 \equiv 2^3 r + 1 \pmod{2^{n+3}}$ for some $r \in \{0, 1, ..., 2^n - 1\}$, the solution set is $\{\pm 2^{e+3}(2^{n+2}t + 2^2 s + 1)\}_{t=0}^{t=2^{e+4}-1}$ for some $s \in \{0, 1, ..., 2^n - 1\}$ such that $(2^2 s + 1)^2 \equiv 2^3 r + 1 \pmod{2^n + 3}$. For $n = 0$, we take $r = s = 0$. Let $b_t = 2^{e+3} + t_1 2^{e+5} + t 2^{e+s-2}$ and

$$
\begin{aligned}
c_t = \frac{Dd - b_t^2}{4 \cdot 2^{2e+7+n}} &= \frac{2^{2e+6}\frac{m_1}{2}\frac{m_2}{2}m^2 - [2^{e+3}(2^{n+2}t + 2^2 s + 1)]^2}{2^{2e+9+n}} \\
&= \frac{\frac{m_1}{2}\frac{m_2}{2}m^2 - (2^{n+2}t + 2^2 s + 1)^2}{2^{n+3}} \\
&= \frac{\frac{m_1}{2}\frac{m_2}{2}m^2 - 2^{2n+4}t^2 - 2^{n+3}(4s+1)t - (4s+1)^2}{2^{n+3}} \\
&= \frac{\frac{m_1}{2}\frac{m_2}{2}m^2 - (4s+1)^2}{2^{n+3}} - 2^{n+1}t^2 - (4s+1)t \\
&= c_0 - 2^{n+1}t^2 - (4s+1)t.
\end{aligned}
$$

Then, we have

$$
\begin{aligned}
N_{D,d}(2^{2e+7+n}) &= \sum_{t=0}^{2^{e+4}-1} \chi_d([-2^{2e+7+n}, b_t, c_t]) \\
&= \begin{cases} \sum_{t=0}^{2^{e+4}-1} \left(\frac{-\frac{m_1}{2}}{-2^{2e+7+n}}\right)\left(\frac{-8}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4, \\ \sum_{t=0}^{2^{e+4}-1} \left(\frac{\frac{m_1}{2}}{-2^{2e+7+n}}\right)\left(\frac{8}{c_t}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4 \end{cases} \\
&= \begin{cases} \left(\frac{-\frac{m_1}{2}}{-2^{n+1}}\right) \sum_{t=0}^{2^{e+4}-1} (-1)^{\frac{c_t'-1}{2}} \left(\frac{c_t}{2}\right) & \text{if } \frac{m_1}{2} \equiv 3 \pmod 4, \\ \left(\frac{\frac{m_1}{2}}{-2^{n+1}}\right) \sum_{t=0}^{2^{e+4}-1} \left(\frac{c_t}{2}\right) & \text{if } \frac{m_1}{2} \equiv 1 \pmod 4. \end{cases}
\end{aligned}
$$

The notation c_t' means the odd part of c_t.

If $\frac{m_1}{2} \equiv 1 \pmod 4$,

$$
\begin{aligned}
\sum_{t=0}^{2^{e+4}-1} \left(\frac{c_t}{2}\right) = \sum_{t=0}^{2^{e+4}-1} & \left(\frac{c_0 - 2^{n+1}t^2 - (4s+1)t}{2}\right) \\
=2^{e+1} \Big[& \left(\frac{c_0}{2}\right) + \left(\frac{c_0 - 2^{n+1} - 4s - 1}{2}\right) + \left(\frac{c_0 - 2}{2}\right) + \left(\frac{c_0 - 2^{n+1} - 4s - 3}{2}\right) \\
& + \left(\frac{c_0 - 4}{2}\right) + \left(\frac{c_0 - 2^{n+1} - 4s - 5}{2}\right) + \left(\frac{c_0 - 6}{2}\right) + \left(\frac{c_0 - 2^{n+1} - 4s - 7}{2}\right) \Big] \\
=0. &
\end{aligned}
$$

Consider $\frac{m_1}{2} \equiv 3 \pmod 4$. If c_0 is odd, we only need to sum over even t.

$$
\begin{aligned}
\sum_{t=0}^{2^{e+4}-1} (-1)^{\frac{c_t'-1}{2}} \left(\frac{c_t}{2}\right) &= \sum_{t=0,2,\ldots,2^{e+4}-2} (-1)^{\frac{c_0 - 2^{n+1}t^2 - 4st - t - 1}{2}} \left(\frac{c_0 - 2^{n+1}t^2 - 4st - t}{2}\right) \\
&=(-1)^{\frac{c_0-1}{2}} \sum_{t=0,2,\ldots,2^{e+4}-2} (-1)^{-\frac{t}{2}} \left(\frac{c_0 - 2^{n+1}t^2 - 4st - t}{2}\right) \\
&=(-1)^{\frac{c_0-1}{2}} 2^{e+1} \Big[\left(\frac{c_0}{2}\right) - \left(\frac{c_0 - 2}{2}\right) + \left(\frac{c_0 - 4}{2}\right) - \left(\frac{c_0 - 6}{2}\right) \Big] \\
&=0.
\end{aligned}
$$

If c_0 is even, we only need to sum over odd t.

$$
\begin{aligned}
\sum_{t=0}^{2^{e+4}-1} (-1)^{\frac{c_t'-1}{2}} \left(\frac{c_t}{2}\right) =& \sum_{t=1,3,\ldots,2^{e+4}-1} (-1)^{\frac{c_0-2^{n+1}t^2-4st-t-1}{2}} \left(\frac{c_0-2^{n+1}t^2-4st-t}{2}\right) \\
=&(-1)^{\frac{c_0}{2}} \sum_{t=1,3,\ldots,2^{e+4}-1} (-1)^{\frac{2^{n+1}t^2+t+1}{2}} \left(\frac{c_0-2^{n+1}t^2-4st-t}{2}\right) \\
=&(-1)^{\frac{c_0}{2}} \sum_{t=1,3,\ldots,2^{e+4}-1} (-1)^{\frac{t+1}{2}+2^n t^2} \left(\frac{c_0-2^{n+1}t^2-4st-t}{2}\right) \\
=&(-1)^{\frac{c_0}{2}+r(n)} \sum_{t=1,3,\ldots,2^{e+4}-1} (-1)^{\frac{t+1}{2}} \left(\frac{c_0-2^{n+1}t^2-4st-t}{2}\right) \\
&\text{(where } r(0)=1 \text{ and } r(n)=0 \text{ for } n\geq 1) \\
=&(-1)^{\frac{c_0}{2}+r(n)} 2^{e+1}\Big[-\left(\frac{c_0-1-4t_1-2^{s-6}}{2}\right)+\left(\frac{c_0-3-4t_1-2^{s-6}}{2}\right) \\
&-\left(\frac{c_0-5-4t_1-2^{s-6}}{2}\right)+\left(\frac{c_0-7-4t_1-2^{s-6}}{2}\right)\Big] \\
=&0.
\end{aligned}
$$

Thus, $N_{D,d}(2^{2e+7+n})=0$ for $n\geq 0$. $\square$

2.5 Proof of Theorem 2.2

Proof. The statement follows easily from

$$F_{1,D,d}(x+1)=F_{1,D,d}(x), \tag{2.21}$$

$$F_{1,D,d}(0)=0 \tag{2.22}$$

and

$$F_{1,D,d}\left(\frac{1}{x}\right)=F_{1,D,d}(x) \tag{2.23}$$

for every $x\in\mathbb{Q}$.

It is easy to verify that (2.21) holds.

In order to check (2.22), notice that

$$\sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ a<0<c}} \chi_d([a,b,c]) = \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3\\ b^2-4ac=Dd\\ c<0<a}} \chi_d([a,b,c])=0 \tag{2.24}$$

since if $[a,b,c]$ appears in the sum, so does $[-c,b,-a]$ and $\chi_d([a,b,c]) = -\chi_d([-a,-b,-c]) =$

$-\chi_d([-c, b, -a])$. Equation (2.22) follows immediately because the first sum equals $F_{1,D,d}(0)$.

We now prove (2.23). We start with a transformation of $F_{1,D,d}(1/x)$:

$$\begin{aligned}
F_{1,D,d}\left(\frac{1}{x}\right) &= \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ a<0 \\ Q\left(\frac{1}{x}\right)>0}} \chi_d([a,b,c]) \\
&= \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ a<0 \\ a\left(\frac{1}{x}\right)^2+b\left(\frac{1}{x}\right)+c>0}} \chi_d([a,b,c]) \\
&= \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ a<0 \\ a+bx+cx^2>0}} \chi_d([a,b,c]) \\
&= \sum_{\substack{Q=[c,b,a]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ c<0 \\ ax^2+bx+c>0}} \chi_d([c,b,a]) \qquad \text{(switched the names a and c)} \\
&= \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ c<0 \\ ax^2+bx+c>0}} \chi_d([a,b,c]) \qquad \text{(by properties of χ_d).}
\end{aligned}$$

It follows that

$$
\begin{aligned}
&F_{1,D,d}\left(\frac{1}{x}\right) - F_{1,D,d}(x) \\
&= \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ c<0 \\ ax^2+bx+c>0}} \chi_d([a,b,c]) - \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ a<0 \\ ax^2+bx+c>0}} \chi_d([a,b,c]) \\
&= \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ c<0<a \\ ax^2+bx+c>0}} \chi_d([a,b,c]) - \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ a<0<c \\ ax^2+bx+c>0}} \chi_d([a,b,c]) \qquad (ac \neq 0 \text{ since } Dd \text{ is not a square}) \\
&= \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ c<0<a \\ ax^2+bx+c>0}} \chi_d([a,b,c]) + \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ -a>0>-c \\ -ax^2-bx-c<0}} \chi_d([-a,-b,-c]) \\
&= \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ c<0<a \\ ax^2+bx+c>0}} \chi_d([a,b,c]) + \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ a>0>c \\ ax^2+bx+c<0}} \chi_d([a,b,c]) \qquad \begin{array}{l}(\text{replaced } -a,-b,-c \text{ by } a,b,c \\ \text{in the second sum})\end{array} \\
&= \sum_{\substack{Q=[a,b,c]\in\mathbb{Z}^3 \\ b^2-4ac=Dd \\ c<0<a}} \chi_d([a,b,c]) \qquad (ax^2+bx+c \neq 0 \text{ since } Dd \text{ is not a square}) \\
&= 0 \text{ by } (2.24)
\end{aligned}
$$

as required. □

CHAPTER 3
FARKAS' IDENTITIES WITH QUARTIC CHARACTERS

3.1 Introduction

In 2004, Farkas [6] introduced an arithmetic function, denoted by $\delta_F(n)$, which is defined as the difference between the number of positive divisors of n that are congruent to 1 and -1 mod 3. He proved that for all positive integers n,

$$\delta_F(n) + 3\sum_{j=1}^{n-1} \delta_F(j)\delta_F(n-j) = \sigma_3'(n), \tag{3.1}$$

where $\sigma_3'(n) = \sum_{\substack{d|n \\ 3\nmid d}} d$.

This identity attracted interest, and was generalized in various directions by several authors. For a Dirichlet character χ, define a function on positive integers by

$$\delta_\chi(n) = \sum_{d|n} \chi(d). \tag{3.2}$$

Then

$$\delta_F(n) = \delta_\chi(n)$$

when χ is the quadratic character modulo 3. Recently K. Williams in [18] used elementary combinatorial arguments to prove 12 identities similar to (3.1) while somehow less elegant. In these identities, the function δ_χ is associated with odd quadratic Dirichlet characters of small conductor such as $3, 4, 8$ and 11. In order to keep our identities as elegant as Farkas' original identity, we stick to characters χ of prime conductor.

It is convenient to define the quantities $\delta_F(0) = 1/6$ and $\sigma_3'(0) = -1/12$ so that Farkas' identity (3.1) becomes

$$\sum_{j=0}^{n-1} \delta_F(j)\delta_F(n-j) = \frac{1}{3}\sigma_3'(n) \tag{3.3}$$

for $n \geq 0$. For an odd quadratic character modulo a prime $p \equiv 3 \pmod 4$, P. Guerzhoy and W. Raji in [8] proved that an exact analogue of Farkas' identity (3.3) holds if and only if $p = 7$. They defined

$$\sigma_p'(n) = \sum_{\substack{d|n \\ p\nmid d}} d \tag{3.4}$$

and rewrote Farkas' identity as an identity between generating functions of $\delta_\chi(n)$ and $\sigma'_p(n)$

$$\left(\sum_{n=0}^{\infty}\delta_\chi(n)q^n\right)^2 = \alpha\sum_{n=0}^{\infty}\sigma'_p(n)q^n, \tag{3.5}$$

for some complex number α. In that way, if one proves the identity (3.5), Farkas' identity

$$\sum_{j=0}^{n}\delta_\chi(j)\delta_\chi(n-j) = \alpha\sigma'_p(n) \text{ for } n \geq 0 \tag{3.6}$$

follows by comparing the coefficients in both sides of (3.5).

The proof that the identity (3.5) holds for $p = 3$ or 7 is easy. Let $G_{1,\chi}$ be the generating function of δ_χ and G_2 be the generation function of σ'_p, i.e.,

$$G_{1,\chi} = \sum_{n=0}^{\infty}\delta_\chi(n)q^n \text{ and } G_2 = \sum_{n=0}^{\infty}\sigma'_p(n)q^n.$$

It is known (see [11] and [12]) that

$$G_{1,\chi} \in M_1(p,\chi) \text{ and } G_2 \in M_2(p).$$

Thus, both $G_{1,\chi}^2$ and G_2 lie in the same space $M_2(p)$. When $p = 3$ and 7, we have $\dim M_2(p) = 1$ (see Proposition A.1) and thus

$$G_{1,\chi}^2 = \alpha G_2$$

for some complex number α. When $p > 7$, we have $\dim M_2(p) > 1$ because the subspace of cusp forms is non-zero. The modular form G_2 is always in the one-dimensional Eisenstein subspace, but now $G_{1,\chi}^2$ is not guaranteed to be in the Eisenstein subspace. Heuristically, the chance of $G_{1,\chi}^2$ lying in the Eisenstein subspace is getting less and less when the dimension of the subspace of cusp forms increases as p increases. However, it is, of course, not a proof for the non-existence of the identity (3.5) for $p > 7$. The proof must be more complicated, in particlar, because it leads to a non-trivial corollary (see [8, Theorem 4]) about non-vanishing of the central special values of L-functions related to modular forms.

The modular forms interpretation of Farkas' identities introduced by Guerzhoy and Raji requires the character χ to be odd. Since they consider quadratic characters of prime conductor, these primes were congruent to 3 modulo 4. We want to consider other primes using a similar approach, therefore we must drop the assumption that χ is quadratic. The next simplest object is a quartic (of exact order four) character χ, and since we want this character to have a prime conductor p and to be odd, we must have $p \equiv 5 \pmod 8$. For such a character χ, we denote by $\bar{\chi}$ its complex conjugate. A direct generalization of (3.5) is

$$\left(\sum_{n=0}^{\infty} \delta_{\chi}(n) q^n\right) \left(\sum_{n=0}^{\infty} \delta_{\overline{\chi}}(n) q^n\right) = \alpha \sum_{n=0}^{\infty} \sigma'_p(n) q^n. \tag{3.7}$$

(for quadratic, therefore real, χ, we have that $\chi = \bar{\chi}$).

Equivalently, equating like powers of q in (3.7), we obtain a direct generalization of (3.6) for a quartic character χ modulo p

$$\sum_{j=0}^{n} \delta_{\chi}(j) \delta_{\overline{\chi}}(n-j) = \alpha \sigma'_p(n) \text{ for } n \geq 0. \tag{3.8}$$

In Section 3.2 we prove the following direct analogue of the principal result from [8].

Theorem 3.1. *Let $p \equiv 5 \pmod 8$ be a prime, and let χ be a quartic Dirichlet character modulo p. The equivalent identities (3.7), (3.8) hold exactly in the following two cases.*
- *$p = 5$. In this case $\alpha = 3/5$.*
- *$p = 13$. In this case $\alpha = 1$.*

While the proof of the identities is easy and similar to that in [8], the proof of their absence for $p > 13$ requires a different approach. Our new approach is also applicable to the setting considered in [8], and we produce another proof of the principal result from [8].

We illustrate the non-triviality of the fact that identities do not hold for $p > 13$ with the following corollary from this fact which is also proved in Section 3.2.

Corollary 3.2. *For every prime $p > 13$ satisfying $p \equiv 5 \pmod 8$, and any quartic Dirichlet character χ modulo p, there exists a cusp Hecke eigenform $f \in S_2(p)$ such that*

$$L(1, f)L(1, f, \chi) \neq 0.$$

Besides (3.7), there is another generalization of (3.6) to the case when the character χ is not real: one can simply square the generating function $\sum_{n=0}^{\infty} \delta_{\chi}(n) q^n$ instead of multiplying it by its conjugate. Interestingly, similar, though quite different identities (see (3.29) and (3.32) below) do hold again exactly in the same cases, namely $p = 5$, and 13. We formulate and prove this result in Section 3.3.

Our interpretation of Farkas' identity and its various generalizations requires χ to be an odd Dirichlet character. Numerical evidence indicates that no similar identities hold true when χ is an even character. We obtained the following theoretical result in this direction.

Theorem 3.3. *For a prime $p = 2q+1$ where q is prime and $q \equiv 1 \pmod 4$, the equivalent identities (3.7) and (3.8) do not hold for any even Dirichlet character modulo p.*

The proof of Theorem 3.3 will be given in Section 3.4.

3.2 Proofs of the main facts

First of all, let us quote the following proposition, theorem and corollary from [8].

Proposition 3.4. *Let p be a prime congruent to 3 modulo 4 and χ be a Dirichlet character modulo p. If for a complex number α,*

$$\left(\sum_{n=0}^{\infty} \delta_\chi(n) q^n\right)^2 = \alpha \sum_{n=0}^{\infty} \sigma'_p(n) q^n, \tag{3.9}$$

then

$$\delta_\chi(0) = -\frac{1}{2p} \sum_{a=1}^{p-1} \chi(a) a, \tag{3.10}$$

$$\sigma'_p(0) = \frac{p-1}{24} \tag{3.11}$$

and $\alpha = \delta_\chi(0)^2 / \sigma'_p(0)$.

Rewriting the formal power series identity (3.9) as identities for their coefficients, we get

$$\sum_{j=0}^{n} \delta_\chi(j) \delta_\chi(n-j) = \alpha \sigma'_p(n) \text{ for } n \geq 0. \tag{3.12}$$

Theorem 3.5. *The equivalent identities (3.9) and (3.12) hold exactly in the following two cases.*
- $p = 3$. *In this case $\alpha = 1/3$, and the identities reduce to the original Farkas' identity.*
- $p = 7$. *In this case $\alpha = 1$.*

In [8], the proof that the identity (3.9) does not hold for $p > 7$ uses a bound on class numbers of quadratic number fields. Here we give a simple proof of this fact without using class numbers of quadratic number fields.

Proof. Assume (3.9) holds for $p > 7$. Equate the coefficients of q in (3.9) to obtain

$$2\delta_\chi(1) 2\delta_\chi(0) = \frac{\delta_\chi(0)^2}{\sigma'_p(0)} \sigma'_p(1).$$

We have $\delta_\chi(1) = \sigma'_p(1) = 1$ and $\sigma'_p(0) = \frac{p-1}{24}$. After simplifying the equation, we have

$$\delta_\chi(0) = \frac{p-1}{12}.$$

Now we equate the coefficients of q^2 in (3.9) to obtain

$$2\delta_\chi(2)\delta_\chi(0) + \delta_\chi(1)\delta_\chi(1) = \frac{\delta_\chi(0)^2}{\sigma'_p(0)}\sigma'_p(2).$$

We have $\delta_\chi(2) = 1 + \chi(2) = 1 + \left(\frac{-p}{2}\right)$ and $\sigma'_p(2) = 3$. Thus, the equation becomes

$$2\left[1 + \left(\frac{-p}{2}\right)\right]\delta_\chi(0) + 1 = \delta_\chi(0)^2 \cdot \frac{24}{p-1} \cdot 3.$$

Now plug in $\delta_\chi(0) = \frac{p-1}{12}$ and simplify. Then we obtain

$$\left[1 + \left(\frac{-p}{2}\right)\right]\frac{p-1}{6} + 1 = \frac{p-1}{2}.$$

If $p \equiv 3 \pmod 8$, then $\left(\frac{-p}{2}\right) = -1$ and $p = 3$. If $p \equiv 7 \pmod 8$, then $\left(\frac{-p}{2}\right) = 1$ and $p = 7$. □

Then, we have the following corollary.

Corollary 3.6. *For every prime $p > 7$ satisfying $p \equiv 3 \pmod 4$, and the quadratic Dirichlet character χ modulo p, there exists a cusp Hecke eigenform $f \in S_2(p)$ such that*

$$L(1, f)L(1, f, \chi) \neq 0.$$

For the proof of Proposition 3.4 and Corollary 3.6, see [8].

Now, before we prove Theorem 3.1, we will prove the following proposition which is an analogue of Proposition 3.4.

Proposition 3.7. *Let p be a prime congruent to 5 modulo 8 and χ be a Dirichlet character modulo p. If for a complex number α,*

$$\left(\sum_{n=0}^{\infty}\delta_\chi(n)q^n\right)\left(\sum_{n=0}^{\infty}\delta_{\overline{\chi}}(n)q^n\right) = \alpha\sum_{n=0}^{\infty}\sigma'_p(n)q^n, \tag{3.13}$$

then

$$\delta_\chi(0) = -\frac{1}{2p}\sum_{a=1}^{p-1}\chi(a)a, \tag{3.14}$$

$$\sigma'_p(0) = \frac{p-1}{24} \tag{3.15}$$

and $\alpha = |\delta_\chi(0)|^2/\sigma'_p(0)$.

Proof. It is known (see [11]) that the series

$$G_{1,\chi} = -\frac{1}{2p}\sum_{a=1}^{p-1}\chi(a)a + \sum_{n\geq 1}\delta_\chi(n)q^n$$

is the Fourier expansion of a modular form which belongs to $M_1(p,\chi)$. Denote $A = -\frac{1}{2p}\sum_{a=1}^{p-1}\chi(a)a$. It is also known (see [12]) that the series

$$G_2 = \frac{p-1}{24} + \sum_{n\geq 1}\sigma_p'(n)q^n$$

is the Fourier expansion of a modular form which belongs to $M_2(p)$. Denote $B = \frac{p-1}{24}$. Assume that (3.13) holds for some $\alpha \in \mathbb{C}$ and with $\delta_\chi(0)$ and $\sigma_p'(0)$ not necessarily given by the formulas (3.14), (3.15), namely

$$(G_{1,\chi} - A + \delta_\chi(0))(G_{1,\overline{\chi}} - \overline{A} + \delta_{\overline{\chi}}(0)) = \alpha(G_2 - B + \sigma_p'(0)). \tag{3.16}$$

Note that $\delta_{\overline{\chi}}(0) = \overline{\delta_\chi(0)}$. After rearranging (3.16), we obtain

$$(G_{1,\chi}G_{1,\overline{\chi}} - \alpha G_2) + (\delta_\chi(0) - A)G_{1,\overline{\chi}} + (\delta_{\overline{\chi}}(0) - \overline{A})G_{1,\chi} = \alpha(\sigma_p'(0) - B) - |A - \delta_\chi(0)|^2.$$

Since χ and $\overline{\chi}$ are conjugates, the product $\chi\overline{\chi}$ is equal to the principal character. Thus $G_{1,\chi}G_{1,\overline{\chi}} \in M_2(p)$. Therefore, $G_{1,\chi}G_{1,\overline{\chi}} - \alpha G_2 \in M_2(p)$. However, $(\delta_\chi(0) - A)G_{1,\overline{\chi}} \in M_1(p,\overline{\chi})$ and $(\delta_{\overline{\chi}}(0) - \overline{A})G_{1,\chi} \in M_1(p,\chi)$. The latter two forms belong to the same space of modular forms of weight 1 with a smaller congruence subgroup, namely $(\delta_\chi(0)-A)G_{1,\overline{\chi}} + (\delta_{\overline{\chi}}(0)-\overline{A})G_{1,\chi} \in M_1(\Gamma_1(p))$. Thus, we have a sum of two forms of different weights which is equal to a constant. That only happens when both forms are zero. Thus, we have $(\delta_\chi(0) - A)G_{1,\overline{\chi}} = -(\delta_{\overline{\chi}}(0) - \overline{A})G_{1,\chi}$. That implies $A = \delta_\chi(0)$ because $(\delta_\chi(0) - A)G_{1,\overline{\chi}}$ and $-(\delta_{\overline{\chi}}(0) - \overline{A})G_{1,\chi}$ are in different subspaces of $M_1(\Gamma_1(p))$ and cannot be constant multiples of each other unless they are zero. This establishes (3.14), (3.15) and the claim about α follows when comparing the constant terms of (3.13). □

Now, we give the proof of Theorem 3.1.

Proof. We first prove (3.13) holds for $p = 5$ or 13. We know that $G_{1,\chi} \in M_1(p,\chi)$ and $G_{1,\overline{\chi}} \in M_1(p,\overline{\chi})$. Therefore, $G_{1,\chi}G_{1,\overline{\chi}} \in M_2(p)$, as well as G_2. When $p = 5$ or 13, the dimension of $M_2(p)$ is one (see Proposition A.1). Thus, the identity (3.13) must be true for some complex number α. After comparing some coefficients in the identity (3.13), we found that $\alpha = 3/5$ when $p = 5$ and $\alpha = 1$ when $p = 13$.

Now we prove the identity (3.13) does not hold for all $n \geq 1$ if $p > 13$. We actually shall show that if $p > 13$, the identity (3.13) already cannot hold simultaneously for $n = 1$ and $n = 2$. For

$n = 1$, the identity reads

$$\delta_\chi(1)\delta_{\overline{\chi}}(0) + \delta_\chi(0)\delta_{\overline{\chi}}(1) = \frac{|\delta_\chi(0)|^2}{\sigma_p'(0)}\sigma_p'(1). \tag{3.17}$$

Note that $\delta_\chi(1) = \sigma_p'(1) = 1$ and $\sigma_p'(0) = \frac{p-1}{2}$. We abbreviate

$$\delta_\chi(0) = -\frac{1}{2p}\sum_{a=1}^{p-1}\chi(a)a = \frac{L}{2} \in \mathbb{Q}(i),$$

where $L = L(0,\chi)$ (see [1, Theorem 12.20]). Substitute all these quantities and into (3.17), we can derive the equality

$$\frac{p-1}{6} \cdot \Re(L) = |L|^2 \tag{3.18}$$

For $n = 2$, the identity (3.13) reads

$$\delta_\chi(2)\delta_{\overline{\chi}}(0) + \delta_\chi(1)\delta_{\overline{\chi}}(1) + \delta_\chi(0)\delta_{\overline{\chi}}(2) = \frac{|\delta_\chi(0)|^2}{\sigma_p'(0)}\sigma_p'(2). \tag{3.19}$$

Note that the modulo p character χ^2 must be a non-trivial quadratic character modulo p, therefore χ^2 must coincide with Kronecker symbol. In particular,

$$\chi^2(2) = \left(\frac{p}{2}\right) = -1$$

since $p \equiv 5 \pmod 8$, and therefore

$$\chi(2) = \pm i.$$

Since obviously $\sigma_p'(2) = 3$, our indentity for $n = 2$ transforms to

$$\frac{p-1}{18}\left[\Re(L) \pm \Im(L) + 1\right] = |L|^2. \tag{3.20}$$

Now, equating (3.18) and (3.20), we get $\Im(L) = \pm[2\Re(L) - 1]$. Denote $R = \Re(L)$ and note that $R \in \mathbb{Q}$ since $L \in \mathbb{Q}(i)$. We thus have

$$L(0,\chi) = R \pm (2R-1)i$$

and equation (3.18) now becomes

$$\frac{p-1}{6} \cdot R = R^2 + (2R-1)^2$$

which transforms to

$$30R^2 - (p+23)R + 6 = 0. \tag{3.21}$$

Since a rational R satisfies this quadratic equation, its discriminant $(p+23)^2 - 4(30)(6) = (p+23)^2 - 720$ being an integer, must be a perfect square, that is

$$(p+23)^2 - 720 = x^2,$$

with a positive integer x. Equivalently,

$$(p+23+x)(p+23-x) = 720.$$

We look at all different factorizations of 720 into a product of two positive integers and find all possible values of p and x. We find that $p = 5$ and $p = 13$ are the only possibilities. □

Before we prove Corollary 3.2, we will prove the following two theorems which are analogues of Theorem 2 and Theorem 3 in [8]. As it is observed in [8, Theorem 2], identity (3.13), though it never holds except for the two primes, is always not far from being true: the orders of magnitude of the left and right hand sides are the same. That happens because the obstruction for these identities to hold comes from cusp forms whose Fourier coefficients grow slower than those of Eisenstein series. In order to formulate a precise result, abbreviate the left-hand sides of our identities:

$$\mathcal{F}_\chi(n) = \sum_{j=0}^{n} \delta_\chi(j)\delta_{\overline{\chi}}(n-j).$$

Theorem 3.8. *Let p be a prime congruent to* 5 *modulo* 8*. Let χ be a quartic Dirichlet character modulo p. For $(p,n) = 1$,*

$$\lim_{n\to\infty} \frac{\mathcal{F}_\chi(n)}{\sigma_p'(n)} = \frac{|\delta_\chi(0)|^2}{\sigma_p'(0)}.$$

Proof. Since $G_{1,\chi}G_{1,\overline{\chi}} \in M_2(p)$ and $M_2(p) = E_2(p) \oplus S_2(p)$, we may write

$$G_{1,\chi}G_{1,\overline{\chi}} = \alpha G_2 + f \tag{3.22}$$

with $\alpha = \frac{|\delta_\chi(0)|^2}{\sigma_p'(0)}$, $G_2 \in E_2(p)$ and $f \in S_2(p)$. Let $f = \sum_{n>0} a(n)q^n$. Equating the coefficients of q^n, we obtain for $n \geq 0$

$$\mathcal{F}_\chi(n) = \alpha\sigma_p'(n) + a(n). \tag{3.23}$$

We can see that $\sigma_p'(n) > n$ if $(p,n) = 1$ from the definition. Now we need an upper bound for the Fourier coefficients of cusp forms. The Ramanujan-Petersson conjecture (see [12]) proved by

Deligne implies that, for n big enough and $(n, p) = 1$,

$$|a(n)| < M\sqrt{n} \tag{3.24}$$

with some constant M. Now, if we divide (3.23) by $\sigma'_p(n)$ and take the limit, the theorem follows. We make a remark that the special case of Ramanujan-Petersson conjecture for weight 2 which we make use of here was proved by Shimura [15]. □

The next theorem gives a generalization of Theorem 3.1 that for $p > 13$, there exist similar identities. This theorem allows us to generate infinitely many similar identities for $p > 13$. Let t_p be the dimension of $S_2(p)$.

Theorem 3.9. *Let p be a prime congruent to 5 modulo 8. Let χ be a quartic Dirichlet character modulo p. There exist a set of complex numbers A_i and two sets of positive integers B_i and C_i for $i = 1, ..., 3^{t_p}$ (all three sets depend on p) such that for any positive integer n*

$$\sum_{i=1}^{3^{t_p}} A_i \mathcal{F}_\chi\left(\frac{n}{B_i}C_i\right) = \sigma'_p(n),$$

where we assume

$$\mathcal{F}_\chi\left(\frac{n}{B}C\right) = 0$$

if n is not divisible by B.

Proof. We rewrite (3.22) as an eigenform decomposition

$$G_{1,\chi}G_{1,\overline{\chi}} = \alpha G_2 + \sum_{i=1}^{t_p} \mu_i g_i, \tag{3.25}$$

such that $g_i = \sum_{n\geq 1} c_i(n)q^n$ with $c_i(1) = 1$. We know that G_2 and g_i are simultaneous Hecke eigenforms, i.e., for a prime $\ell \neq p$, the Hecke operator T_ℓ acts on them and we have

$$G_2|T_\ell = (\ell + 1)G_2 \text{ and } g_i|T_\ell = c_i(\ell)g_i.$$

For $p \neq 5$, 13, μ_i are not all zero by Theorem 3.1. Pick j such that $\mu_j \neq 0$. Then choose ℓ such that $c_j(\ell) \neq \ell + 1$ and apply the operator $T_\ell - c_j(\ell)$ to (3.25) to obtain

$$G_{1,\chi}G_{1,\overline{\chi}}|T_l - c_j(l)G_{1,\chi}G_{1,\overline{\chi}} = \alpha' G_2 + \sum_{i=1}^{t_p} \mu'_i g_i$$

with $\alpha' \neq 0$ and $\mu'_j = 0$. Repeat the process. After eliminating the forms g_i one by one, we obtain the claimed identities. □

We give an example of such identity for $p = 37$. We have $\dim S_2(37) = 2$, and the space admits a basis out of two Hecke eigenforms with rational integer coefficients. We make use of the fact that one of these cusp forms has zero Hecke eigenvalues at primes $p_1 = 2$ and 5, while another one has zero Hecke eigenvalues at $p_2 = 17$ and 19. That allows us to produce the identities for $n > 0$:

$$\mathcal{F}_\chi(p_1p_2n) + p_1\mathcal{F}_\chi(p_2n/p_1) + p_2\mathcal{F}_\chi(p_1n/p_2) + p_1p_2\mathcal{F}(n/(p_1p_2)) = \frac{1 + p_1 + p_2 + p_1p_2}{3}\sigma'_{37}(n),$$

where χ is a quartic character modulo 37, and one may pick any $p_1 \in \{2, 5\}$ and $p_2 \in \{17, 19\}$.

Now, we prove Corollary 3.2.

Proof. For $f \in S_2(p)$ with q-expansion $f(\tau) = \sum_{n\geq 1} b(n)q^n$, we write $f_\rho(\tau) = \overline{f(-\overline{\tau})} = \sum_{n\geq 1} \overline{b(n)}q^n$. It is known that $f_\rho \in S_2(p)$. Also, it is known that if f is a Hecke eigenform, then so is f_ρ. Since $p > 13$, Theorem 3.1 implies that there exists j such that $\mu_j \neq 0$ in decomposition (3.25). Put $f_\rho = g_j$. Take the Petersson scalar product of both sides of (3.25) with f_ρ. Since the scalar product is Hermitian, we have on the right hand side

$$\left\langle f_\rho, \alpha G_2 + \sum_{i=1}^{t_p} \mu_i g_i \right\rangle = \overline{\mu_j}\langle f_\rho, f_\rho\rangle \neq 0. \tag{3.26}$$

On the other side, the Rankin method (see [16]) implies

$$\langle f_\rho, G_{1,\chi}G_{1,\overline{\chi}}\rangle = \Omega L(1, f)L(1, f, \chi)$$

with some $\Omega \in \mathbb{C}$. Now the result follows. □

3.3 Squaring the generating function of δ_χ

As mentioned in the introduction, we may also consider squaring the generating function of δ_χ. To do this, for any $n \geq 1$, we define

$$\tilde{\sigma}_p(n) = \sum_{0<d|n} \left(\frac{p}{d}\right) d. \tag{3.27}$$

and

$$\hat{\sigma}_p(n) = \sum_{0<d|n} \left(\frac{p}{d}\right) n/d \tag{3.28}$$

Proposition 3.10. *Let p be a prime congruent to 5 modulo 8, χ be a Dirichlet character modulo p and $\psi = \chi^2 = \left(\frac{p}{\cdot}\right)$. If for complex numbers α' and β',*

$$\left(\sum_{n=0}^{\infty} \delta_\chi(n)q^n\right)^2 = \alpha' \sum_{n=0}^{\infty} \tilde{\sigma}_p(n)q^n + \beta' \sum_{n=1}^{\infty} \hat{\sigma}_p(n)q^n, \tag{3.29}$$

then

$$\delta_\chi(0) = -\frac{1}{2p}\sum_{a=1}^{p-1}\chi(a)a, \tag{3.30}$$

$$\tilde{\sigma}_p(0) = -\frac{1}{4}B_{2,\psi} \tag{3.31}$$

and $\alpha' = \delta_\chi(0)^2/\tilde{\sigma}_p(0)$, $\beta' = \frac{2\delta_\chi(0)\delta_\chi(1)-\alpha\tilde{\sigma}_p(1)}{\hat{\sigma}_p(1)} = 2\delta_\chi(0) - \alpha$.

Proof. As mentioned in Proposition 3.7, the series

$$G_{1,\chi} = -\frac{1}{2p}\sum_{a=1}^{p-1}\chi(a)a + \sum_{n\geq 1}\delta_\chi(n)q^n$$

is the Fourier expansion of a modular form which belongs to $M_1(p,\chi)$. Denote $A = -\frac{1}{2p}\sum_{a=1}^{p-1}\chi(a)a$. It is also known (see [11] and [12]) that the series

$$\tilde{E}_{2,p} = -\frac{1}{4}B_{2,\psi} + \sum_{n\geq 1}\tilde{\sigma}_p(n)q^n$$

and

$$\hat{E}_{2,p} = \sum_{n\geq 1}\hat{\sigma}_p(n)q^n$$

are the Fourier expansions of modular forms which belong to $M_2(p,\psi)$. Denote $B = -\frac{1}{4}B_{2,\psi}$. Assume that (3.29) holds for some $\alpha', \beta' \in \mathbb{C}$ with $\delta_p(0)$ and $\tilde{\sigma}_p(0)$ not necessarily given by the formulas (3.30), (3.31), namely

$$[G_{1,\chi} - A + \delta_\chi(0)]^2 = \alpha'[\tilde{E}_{2,p} - B + \tilde{\sigma}_p(0)] + \beta'\hat{E}_{2,p}.$$

After rearranging, we obtain

$$(G_{1,\chi}^2 - \alpha'\tilde{E}_{2,p} - \beta'\hat{E}_{2,p}) + 2[\delta_\chi(0) - A]G_{1,\chi} = \alpha'[\tilde{\sigma}_p(0) - B] - [\delta_\chi(0) - A]^2.$$

Now, we have $G_{1,\chi}^2 \in M_2(p,\psi)$. Therefore, $G_{1,\chi}^2 - \alpha'\tilde{E}_{2,p} - \beta'\hat{E}_{2,p} \in M_2(p,\psi)$. However, $2[\delta_\chi(0) - A]G_{1,\chi} \in M_1(p,\chi)$ and $\alpha'[\tilde{\sigma}_p(0) - B] - [\delta_\chi(0) - A]^2$ is a constant. The sum of two modular forms of different weights may be a constant only if both forms are zero. This establishes (3.30), (3.31) and the claim about α' and β' follows when comparing the constant terms and the coefficients of q terms in (3.29). □

To rewrite the formal power series identity (3.29) as identities for their coefficients, for $n \geq 0$, we let

$$\mathcal{H}_\chi(n) = \sum_{j=0}^{n} \delta_\chi(j)\delta_\chi(n-j).$$

Then the identity (3.29) is equivalent to

$$\mathcal{H}_\chi(n) = \sum_{j=0}^{n} \delta_\chi(j)\delta_\chi(n-j) = \alpha\tilde{\sigma}_p(n) + \beta\hat{\sigma}_p(n) \text{ for } n \geq 0. \tag{3.32}$$

Theorem 3.11. *The equivalent identities (3.32), (3.29) hold exactly in the following two cases.*
• $p = 5$. *In this case* $\alpha' = -\frac{4+3\chi(2)}{10}$ *and* $\beta' = \frac{2+\chi(2)}{2}$.
• $p = 13$. *In this case* $\alpha' = -\frac{\chi(2)}{2}$ *and* $\beta' = \frac{2+3\chi(2)}{2}$.

Proof. We first prove (3.29) holds for $p = 5$ or 13. We know that $G_{1,\chi} \in M_1(p, \chi)$. Therefore, $G_{1,\chi}^2 \in M_2(p, \psi)$ where $\psi = \chi^2$. When $p = 5$ or 13, we have $\dim M_2(p, \psi) = 2$ (see Proposition A.1) and the space is generated by $\tilde{E}_{2,p}$ and $\hat{E}_{2,p}$. Thus, the identity (3.29) must be true for some complex numbers α and β. After comparing some coefficients in the identity (3.29), we found that $\alpha' = -\frac{4+3\chi(2)}{10}$ and $\beta' = \frac{2+\chi(2)}{2}$ when $p = 5$, and $\alpha = -\frac{\chi(2)}{2}$ and $\beta = \frac{2+3\chi(2)}{2}$ when $p = 13$.

We will now show that the identity (3.29) does not holds for all $n \geq 0$ if $p > 13$. Specifically, we want to show that, if $p > 13$, the identity cannot hold simultaneously for $n = 2$ and 3.

For $n = 2$, the identity (3.29) reads

$$2\delta_\chi(0)\delta_\chi(2) + \delta_\chi(1)\delta_\chi(1) = \frac{\delta_\chi(0)^2}{\tilde{\sigma}_p(0)}\tilde{\sigma}_p(2) + \frac{2\delta_\chi(0)\delta_\chi(1) - \frac{\delta_\chi(0)^2}{\tilde{\sigma}_p(0)}\tilde{\sigma}_p(1)}{\hat{\sigma}_p(1)}\hat{\sigma}_p(2). \tag{3.33}$$

Note that $\delta_\chi(1) = \tilde{\sigma}_p(1) = \hat{\sigma}_p(1) = 1$, $\delta_\chi(2) = 1\chi(2)$, $\hat{\sigma}_p(2) = 1$ and $\tilde{\sigma}_p(2) = -1$ along with $\tilde{\sigma}_p(0) = -\frac{1}{4}B_{2,\psi}$. Substituting these quantities and into (3.33), we can derive the equality

$$\frac{\delta_\chi(0)^2}{-\frac{1}{4}B_{2,\psi}} = -\chi(2)\delta_\chi(0) - \frac{1}{2}. \tag{3.34}$$

A similar calculation simplifies the identity (3.29) for $n = 3$ to

$$2[1 + \chi(3)]\delta_\chi(0) + 2(1 + \chi(2)) = \frac{\delta_\chi(0)^2}{-\frac{1}{4}B_{2,\psi}}[1 + 3\psi(3)] + \left(2\delta_\chi(0) - \frac{\delta_\chi(0)^2}{-\frac{1}{4}B_{2,\psi}}\right)[3 + \psi(3)], \tag{3.35}$$

and we combine it with (3.34) to obtain

$$2[1+\chi(3)]\delta_\chi(0)+2(1+\chi(2)) = \left(-\chi(2)\delta_\chi(0)-\frac{1}{2}\right)[1+3\psi(3)] + \left(2\delta_\chi(0)+\chi(2)\delta_\chi(0)+\frac{1}{2}\right)[3+\psi(3)]. \tag{3.36}$$

Since χ is a quartic character, $\chi(3) \in \{\pm 1, \pm i\}$. The above equation allows us to find the quantity $\delta_\chi(0)$ which corresponds to every one of these four values. With this quantity, we make use of equation (3.34) to find the corresponding values of $B_{2,\psi}$. These turn out to be either 4, or 4/5, or a complex number which is not rational. However, Proposition 3.12, which we will prove next, says $B_{2,\psi}$ is a rational number bigger than 4. This finishes the proof. □

Proposition 3.12. *For a prime $p \equiv 5 \pmod 8$ with $p > 13$ and the quadratic Dirichlet character ψ modulo p, the generalized Bernoulli number $B_{2,\psi}$ is a rational number bigger than 4. When $p = 5$, $B_{2,\psi} = 4/5$ and when $p = 13$, $B_{2,\psi} = 4$.*

Proof. Let p be a prime congruent to 5 mod 8 and let ψ be a quadratic Dirichlet character modulo p, i.e., $\left(\frac{p}{\cdot}\right)$. Recall from Chapter 1 that Cohen [2] defined a quantity $H(r,N)$ for integers $r \geq 1$ and $N \geq 0$ such that $H(r,N) = L(1-r,\chi_D)$ if $D = (-1)^r N$ is a fundamental discriminant and $\chi_D = \left(\frac{D}{\cdot}\right)$. If we take $r = 2$ and $D = p$, then we have $H(2,p) = L(-1,\psi)$. It is also well-known that $L(-1,\psi) = -\frac{B_{2,\psi}}{2}$ (see [4, Theorem 10.3.1]). Therefore, we have $B_{2,\psi} = -2H(2,p)$. From [2], we know that $H(2,p)$ is a rational number and has the explicit formula,

$$H(2,p) = -\frac{1}{5}\sum_s \sigma_1\left(\frac{p-s^2}{4}\right),$$

where s runs through all integers such that $p - s^2 \geq 0$, and σ_1 is the sum of positive divisors function with $\sigma_1(0) = \frac{1}{2}\zeta(-1)$. Also, if $\frac{p-s^2}{4}$ is not an integer, $\sigma_1(\frac{p-s^2}{4}) = 0$. Since $p \equiv 5 \pmod 8$, if $s = 0$, $\sigma_1\left(\frac{p}{4}\right) = 0$. Also note that s^2 stays the same no matter s is positive or negative. Thus, we can just sum over all positive integers s and then double the sum. In other words, we have $B_{2,\psi} = \frac{4}{5}\sum_{s>0}\sigma_1\left(\frac{p-s^2}{4}\right)$. It is a direct calculation for $p = 5$ and 13 that $B_{2,\psi} = 4/5$ and $B_{2,\psi} = 4$ respectively.

If $p > 13$, then $p \geq 29$, and we have

$$B_{2,\psi} = \frac{4}{5}\sum_{s>0}\sigma_1\left(\frac{p-s^2}{4}\right) \geq \frac{4}{5}\sigma_1\left(\frac{p-1}{4}\right) \geq \frac{4}{5}\sigma_1(7) \geq \frac{32}{5} > 4$$

because $\frac{p-1}{4} \geq 7$ and $\sigma_1\left(\frac{p-1}{4}\right) \geq 1 + 7 = 8$. □

Now, we present the following theorem which is an analogue of Theorem 3.8.

Theorem 3.13. *Let $p \equiv 5 \pmod 8$ and χ be a quartic Dirichlet character modulo p. For $(p,n)=1$,*

$$\lim_{n\to\infty} \frac{\mathcal{H}_\chi(n)}{\tilde{\sigma}_p(n)} = \alpha' + \left(\frac{p}{n}\right)\gamma,$$

with some $\gamma \in \mathbb{C}$.

The proof of this theorem is more subtle both because the will have to deal with two arithmetic functions, $\tilde{\sigma}_p$ and $\hat{\sigma}_p$, instead of just σ'_p, and because the functions themselves are slightly more complicated. We start with a proposition which relates these two functions.

Proposition 3.14. *For a prime p and a positive integer n not divisible by p,*

$$\hat{\sigma}_p(n) = \left(\frac{p}{n}\right)\tilde{\sigma}_p(n).$$

Proof. Since $\hat{\sigma}_p(n)$, $\tilde{\sigma}_p(n)$ and $\left(\frac{p}{n}\right)$ are all multiplicative functions, we only need to consider the case when n is a prime power. Let $n = l^r$ for some prime $l \neq p$ and some positive integer r. By definition, we have

$$\begin{aligned}\hat{\sigma}_p(n) = \hat{\sigma}_p(l^r) &= \sum_{t=0}^{r}\left(\frac{p}{l^t}\right)l^{r-t} = \sum_{t=0}^{r}\left(\frac{p}{l}\right)^t l^{r-t} = \sum_{u=0}^{r}\left(\frac{p}{l}\right)^{r-u} l^u = \left(\frac{p}{l}\right)^r \sum_{u=0}^{r}\left(\frac{p}{l}\right)^{-u} l^u \\ &= \left(\frac{p}{l^r}\right)\sum_{u=0}^{r}\left(\frac{p}{l}\right)^u l^u = \left(\frac{p}{n}\right)\tilde{\sigma}_p(n)\end{aligned}$$

because for a positive integer u

$$\left(\frac{p}{l^u}\right) = \left(\frac{p}{l}\right)^u \quad \text{and} \quad \left(\frac{p}{l}\right)^{-u} = \left(\frac{p}{l}\right)^u,$$

followed from the definition of Kronecker symbol. ☐

We thus have that $|\hat{\sigma}_p(n)| = |\tilde{\sigma}_p(n)|$, for $p \nmid n$. and we will use a lower bound for this quantity given in the next proposition.

Proposition 3.15. *For a positive integer n not divisible by p,*

$$|\tilde{\sigma}_p(n)| \geq n(1/2)^{\omega(n)},$$

where $\omega(n)$ is the number of distinct prime factors of n.

Proof. Since the arithmetic functions $\tilde{\sigma}_p(n)$ and $(1/2)^{\omega(n)}$ are multiplicative, it suffices to prove that, for a prime l and a positive integer r,

$$|\tilde{\sigma}_p(l^r)| \geq \frac{1}{2}l^r.$$

Indeed,

$$|\tilde{\sigma}_p(l^r)| = \left|\sum_{u=0}^{r} \left(\frac{p}{l}\right)^u l^u\right| = \left|\frac{1-\left(\frac{p}{l}\right)^{u+1} l^{u+1}}{1-\left(\frac{p}{l}\right) l}\right| \geq \frac{l^{r+1}-1}{l+1} \geq \frac{1}{2} l^r,$$

where the latter inequality is equivalent to $l \geq 1 + 2l^{-r}$. □

We are now in a position to prove Theorem 3.13.

Proof. Since $G_{1,\chi}^2 \in M_2(p,\psi)$ with

$$\psi(n) = \chi^2(n) = \left(\frac{p}{n}\right),$$

we can write

$$G_{1,\chi}^2 = \alpha' \tilde{E}_{2,p} + \gamma \hat{E}_{2,p} + f \tag{3.37}$$

with some $\gamma \in \mathbb{C}$, a cusp form $f \in S_2(p,\psi)$, and

$$\alpha' = \frac{\delta_\chi(0)^2}{\tilde{\sigma}_p(0)}$$

because neither f not $\hat{G}_{2,\psi}$ has constant term in the Fourier expansion.

We equate the coefficients of q^n, divide both parts of the equation by $\tilde{\sigma}_p(n)$, and use Proposition 3.14 to obtain

$$\frac{\mathcal{H}_\chi(n)}{\tilde{\sigma}_p(n)} = \alpha' + \left(\frac{p}{n}\right)\gamma + \frac{a(n)}{\tilde{\sigma}_p(n)}.$$

In order to finish the proof, it now suffices to show that

$$\lim_{n\to\infty} \frac{a(n)}{\tilde{\sigma}_p(n)} = 0. \tag{3.38}$$

As in part (a) above, we still have that $|a(n)| \leq L\sqrt{n}$ for some constant L, and we make use of Proposition 3.15 to get, for n big enough,

$$\left|\frac{a(n)}{\tilde{\sigma}_p(n)}\right| \leq \frac{L\sqrt{n}}{\left(\frac{1}{2}\right)^{\omega(n)} n} = \frac{L 2^{\omega(n)}}{\sqrt{n}}.$$

We now make use of a bound proved in [14]

$$\omega(n) < 13841 \frac{\ln n}{\ln(\ln n)}$$

to obtain that

$$\left|\frac{a(n)}{\tilde{\sigma}_p(n)}\right| < \frac{L\cdot 2^{13841\frac{\ln n}{\ln(\ln n)}}}{\sqrt{n}} = \frac{L\cdot n^{\frac{13841\ln 2}{\ln\ln n}}}{\sqrt{n}} = L\cdot n^{\frac{13841\ln 2}{\ln\ln n}-\frac{1}{2}} \to 0$$

as $n\to\infty$. That implies (3.38) and concludes the proof. □

The following theorem again says we have infinitely many similar, though less elegant, identities which hold for primes bigger than 13.

Theorem 3.16. *There exist a set of complex numbers A_i, two sets of positive integers B_i and C_i for $i = 1,...,3^{t_p}$ (all three sets depend on p), and two complex numbers, α'' and β'', such that for any positive integer n*

$$\sum_{i=1}^{3^{t_p}} A_i\mathcal{H}_\chi\left(\frac{n}{B_i}C_i\right) = \alpha''\tilde{\sigma}_p(n) + \beta''\hat{\sigma}_p(n),$$

where we assume

$$\mathcal{H}_\chi\left(\frac{n}{B}C\right) = 0$$

if n is not divisible by B.

Proof. The proof is similar to the proof of Theorem 3.9. We rewrite (3.37) as an eigenform decomposition

$$G_{1,\chi}^2 = \alpha'\tilde{E}_{2,p} + \gamma\hat{E}_{2,p} + \sum_{i=1}^{t_p}\mu_i g_i, \tag{3.39}$$

with $g_i = \sum_{n\geq 1} c_i(n)q^n$. For $p\neq 5, 13$, μ_i are not all zero by Theorem 3.11. Pick j such that $\mu_j\neq 0$ and apply the operator $T_l - c_j(l)$, for some prime $l\neq p$, to obtain

$$G_{1,\chi}^2|T_l - c_j(l)G_{1,\chi}^2 = \alpha''\tilde{E}_{2,p} + \beta''\hat{E}_{2,p} + \sum_{i=1}^{t_p}\mu_i' g_i$$

for some complex numbers α'' and β'' with either $\alpha''\neq 0$ or $\beta''\neq 0$ but $\mu_j' = 0$. Repeat the process. After eliminating the forms g_i one by one, we obtain the claimed identities. □

Below is a corollary to Theorem 3.11 about nonvanishing central values of L-functions.

Corollary 3.17. *For every prime $p > 13$ satisfying $p\equiv 5 \pmod 8$, and any quartic Dirichlet character χ modulo p, there exists a cusp Hecke eigenform $f\in S_2(p,\psi)$ with $\psi=\chi^2$ such that*

$$L(1,f)L(1,f,\chi)\neq 0.$$

Proof. For $f\in S_2(p,\psi)$ with q-expansion $f(\tau) = \sum_{n\geq 1} b(n)q^n$, we write $f_\rho(\tau) = \overline{f(-\overline{\tau})} = \sum_{n\geq 1}\overline{b(n)}q^n$. Since $p > 13$, Theorem 3.11 implies that there exists j such that $\mu_j\neq 0$ in the eigenform decomposition $G_{1,\chi}^2 = \alpha'\tilde{E}_{2,p} + \gamma\hat{E}_{2,p} + \sum_{i=1}^{t_p} \mu_i g_i$. Put $f_\rho = g_j$. Take the Petersson scalar product of both sides of (3.39) with f_ρ. Since the scalar product is Hermitian, we have on the right hand side

$$\left\langle f_\rho, \alpha'\tilde{E}_{2,p} + \gamma\hat{E}_{2,p} + \sum_{i=1}^{t_p} \mu_i g_i \right\rangle = \overline{\mu_j}\langle f_\rho, f_\rho\rangle \neq 0. \tag{3.40}$$

On the other side, the Rankin method (see [16]) implies

$$\langle f_\rho, G_{1,\chi}^2\rangle = \Omega L(1,f)L(1,f,\chi)$$

with some $\Omega \in \mathbb{C}$. Now the result follows. □

3.4 Even characters

In this section, we prove Theorem 3.3. We want to prove that, for an even character χ, the identity (3.8) does not hold simultaneously already for $n = 1$ and $n = p$. Specifically, assuming (3.8) is true for $n = 1$, we find that $\alpha = \delta_\chi(0) + \delta_{\bar{\chi}}(0)$, and the identity for $n = p$ simplifies to

$$\sum_{j=1}^{p-1} \delta_\chi(j)\delta_{\bar{\chi}}(p-j) = 0. \tag{3.41}$$

Theorem 3.3 follows immediately from the following proposition.

Proposition 3.18. *Let $p = 2q + 1$ and $q \equiv 1 \pmod 4$ be a prime. Let ψ be an even Dirichlet character modulo p. Then*

$$\sum_{j=1}^{p-1} \delta_\psi(j)\delta_{\bar{\psi}}(p-j) \neq 0. \tag{3.42}$$

The rest of this section is devoted to the proof of Proposition 3.18.

Our following first proposition implies, in particular, that (3.41) is always true if the character χ is odd.

Proposition 3.19. (a) *Let p be a prime and χ be a Dirichlet character modulo p. For any $1 \leq j \leq p-1$, the expression $\delta_\chi(j)\delta_{\overline{\chi}}(p-j)$ is purely imaginary if χ is odd, and real if χ is even.*
(b) *If the character χ is odd, then*

$$\sum_{j=0}^{p-1} \delta_\chi(j)\delta_{\bar{\chi}}(p-j) = 0.$$

Proof. The expression in question can be rewritten as a sum

$$\delta_\chi(j)\delta_{\overline{\chi}}(p-j) = \sum_{d|j}\sum_{d'|p-j}\chi(d)\bar{\chi}(d') = \frac{1}{2}\sum_{d|j,\ d'|(p-j)}\left(\chi(d)\bar{\chi}(d') + \chi(j/d)\bar{\chi}((p-j)/d')\right).$$

Making use of $\chi(j)\bar{\chi}(-j) = \chi(-1)$, we transform every summand

$$\chi(d)\bar{\chi}(d') + \chi(j/d)\bar{\chi}((p-j)/d') = \chi(d)\bar{\chi}(d') + \chi(j)\bar{\chi}(d)\bar{\chi}(-j)\chi(d') = \chi(d)\bar{\chi}(d') + \chi(-1)\overline{\chi(d)\bar{\chi}(d')},$$

and assertion (a) becomes clear term-by-term. Assertion (b) follows from that since the sum is real (because it is equal to its conjugate). □

Our next proposition exploits some specifics of our assumptions about the prime p.

Proposition 3.20. *Let $p = 2q+1$ and $q \equiv 1 \pmod 4$ be a prime. Then 2 is a primitive root modulo p (i.e., a generator of $(\mathbb{Z}/p\mathbb{Z})^*$).*

Proof. The subgroup of squares has index 2 in $(\mathbb{Z}/p\mathbb{Z})^*$, thus there are exactly $(p-1)/2 = q$ non-squares modulo p. At the same time, there are exactly

$$\varphi(\varphi(p)) = \varphi(p-1) = \varphi(2q) = \varphi(2)\varphi(q) = q-1$$

primitive roots modulo p. Since no square can be a primitive root, all but one non-squares must be primitive roots. The non-square which is not a primitive root is -1 (since $p \equiv 3 \mod 4$, the residue -1 is indeed a non-square modulo p). By quadratic reciprocity, 2 is a quadratic non-residue modulo p, and since it is different from -1, it must be a primitive root modulo p. □

From now on we assume that our prime $p = 2q+1$, where $q \equiv 1 \pmod 4$ is a prime, and let $\zeta = \exp(2\pi i/(p-1))$. The group of Dirichlet characters modulo p is cyclic of order $p-1$ generated by the (odd) character χ defined by

$$\chi(2) = \zeta.$$

We now construct certain polynomials associated with a Dirichlet character ξ modulo p. For an arbitrary Dirichlet character ξ modulo p, define integers

$$0 \le t(\xi, d) \le p-2$$

by

$$\xi(d) = \zeta^{t(\xi,d)}.$$

Note that, for any positive integers k and d,

$$t(\xi^k, d) \equiv kt(\xi, d) \mod (p-1). \tag{3.43}$$

For a positive integer $j \le p-1$, let

$$h_{\xi,j}(x) := \sum_{d|j} x^{t(\xi,d)}.$$

The function $h_{\xi,j}(x)$ is a polynomial in x of degree at most $p-2$. Let

$$f_\xi(x) := \sum_{j=1}^{p-1} h_{\xi,j}(x) h_{\bar{\xi},p-j}(x) = b_{2p-4}x^{2p-4} + b_{2p-3}x^{2p-3} + \cdots + b_p x^p + b_{p-1}x^{p-1} + b_{p-2}x^{p-2} + \cdots + b_1 x + b_0$$

be a polynomial of degree at most $2p-4$.

The polynomials just introduced allow us to reformulate Proposition 3.18. Clearly,

$$h_{\xi,j}(\zeta) = \delta_\xi(j),$$

and, for a positive integer k, we use (3.43) to obtain

$$h_{\chi^k,j}(\zeta) = \delta_{\chi^k}(j) = \sum_{d|j} \chi^k(d) = \sum_{d|j} [\chi(d)]^k = \sum_{d|j} [\zeta^{t(\chi,d)}]^k = \sum_{d|j} [\zeta^k]^{t(\chi,d)} = h_{\chi,j}(\zeta^k).$$

It follows that

$$\sum_{j=0}^{p-1} \delta_{\chi^k}(j) \delta_{\bar{\chi}^k}(p-j) = f_{\chi^k}(\zeta) = f_\chi(\zeta^k).$$

Since every Dirichlet character ξ modulo p can be written as $\xi = \chi^k$, where the parity of ξ coincides with the parity of k, we deduce from Proposition 3.19 that $f_\chi(\zeta^k) = 0$ if k is odd, and our target Proposition 3.18 can be reformulated as follows.

Proposition 3.21. *The quantity $\zeta^k = \exp(2k\pi i/(p-1))$ with a positive integer k is a root of the polynomial $f_\chi(x)$ associated as above to the character χ modulo p defined by $\chi(2) = \zeta = \exp(2\pi i/(p-1))$ if and only if k is odd.*

Our ultimate goal now is to prove Proposition 3.21. We need some specific information about the coefficients of $f_\chi(x)$ given in the following proposition.

Proposition 3.22. *The polynomial $f_\chi(x)$ has positive integer coefficients. Furthermore,*

$$b_0 = p-1, \quad b_1 = \frac{p-1}{2} + 1, \quad b_p = b_{p-1} = 0.$$

We postpone the proof of Proposition 3.22 and prove Proposition 3.21 (therefore Proposition 3.18, therefore Theorem 3.3 now).

Proof of Proposition 3.21. Let

$$g(x) = b_{p-2}x^{p-2} + (b_{2p-4} + b_{p-3})x^{p-3} + \cdots + (b_p + b_1)x + (b_{p-1} + b_0).$$

Then $f_\chi(x) - g(x) = h(x)(x^{p-1} - 1)$, and therefore ζ^k is a root of $f_\chi(x)$ if and only if it is a root of $g(x)$. Note the factorization

$$x^{p-1} - 1 = x^{2q} - 1 = (x^q - 1)(x^q + 1)$$

with ζ^k with odd k are exactly the roots of the second factor (while those with even k are exactly the roots of the first factor). Since $f_\chi(\zeta^k) = 0$ if k is odd, we have that

$$g(x) = (x^q + 1)P(x)$$

with a polynomial $P(x)$ with integer coefficients of degree at most $q - 1$. If an even power of ζ was a root of $g(x)$, it would be a root of $P(x)$ thus $P(x)$ would be divisible by the cyclotomic polynomial $\Phi_q(x) = x^{q-1} + x^{q-2} + \cdots + x^2 + x + 1$ because q is a prime. Since, however, $\deg P(x) \leq \deg \Phi(x) = q - 1$, the two polynomials would differ by a constant factor. If this was the case then, for $P(x) = a_{q-1}x^{q-1} + \ldots + a_1x + a_0$, we would have $a_1 = a_0$, which translates immediately to

$$b_p + b_1 = b_{p-1} + b_0$$

for the coefficients of $f_\chi(x)$ in contradiction with Proposition 3.22. □

We are left only to prove Proposition 3.22.

Proof Proposition 3.22. We start with recording some values of the character χ. Since

$$\chi(2) = \zeta,$$

$$\zeta\chi(q) = \chi(2q) = \chi(p-1) = -1 = \zeta^q \quad \text{implies} \quad \chi(q) = \zeta^{q-1};$$

$$\chi(2)\chi(q+1) = \chi(2q+2) = \chi(p+1) = 1 \quad \text{implies} \quad \chi(q+1) = \zeta^{p-2}.$$

We thus have the following values of $t(\chi, d)$:

d	$t(\chi, d)$
1	0
2	1
q	$q-1$
$q+1$	$p-2$

By definition,

$$f_\chi(x) = \sum_{j=1}^{p-1} h_{\chi,j}(x) h_{\bar{\chi},p-j}(x)$$

and since both $h_{\chi,j}(x)$ and $h_{\bar{\chi},p-j}(x)$ have constant terms 1, the constant term of $f_\chi(x)$ is

$$b_0 = p - 1.$$

In order to calculate b_1, note that $h_{\chi,j}(x)$ has an x-term (with coefficient 1) whenever $2|j$, while $h_{\bar{\chi},p-j}(x)$ has an x-term (with coefficient 1) only when $j = q$ (otherwise $(q+1) \nmid (p-j) = 2q+1-j$). We thus have all together

$$b_1 = \frac{p-1}{2} + 1.$$

Note that for every d such that $1 < d \leq p-1$, there exists exactly one solution u such that $1 < u \leq p-1$ and $t(\chi, d) + t(\bar{\chi}, u) = p - 1$, and that is $u = d$ since $\chi(d)\bar{\chi}(d) = 1$. It follows that

$$b_{p-1} = 0$$

because no $d > 1$ can divide simultaneously j and $p - j$.

We now claim that $b_p = 0$. Otherwise we would have that

$$t(\chi, d) + t(\bar{\chi}, y) = p.$$

That implies

$$t(\chi, y) = t(\chi, d) - 1,$$

therefore

$$d \equiv 2y \mod p.$$

Since both $2 \leq d, y \leq p-1$, either $d = 2y$ or $d = 2y - p$ with $y > (p+1)/2$.

However, $d = 2y$ is not possible since $2y|j$ and $y|p-j$ at the same time would imply $y|p$.

We are thus left with the only option that $y|(p-j)$ and $(2y-p)|j$ while $y > (p+1)/2$ which implies $y = p - j$. Then $2y - p = p - 2j$ and we can write

$$(p - 2j)t = j$$

with some positive integer t. We find that

$$j = \frac{pt}{1+2t},$$

and conclude that $p = 2t + 1$ because $(t, 2t + 1) = 1$. Thus

$$(p - 2j)\frac{p - 1}{2} = j,$$

and that implies

$$j = \frac{p - 1}{2} \quad \text{therefore} \quad y = p - j = \frac{p + 1}{2}$$

in contradiction with $y > (p + 1)/2$ above. □

APPENDIX A
DIMENSION

In this section, we compute the dimension of $M_2(p)$ and $M_2(p,\psi)$ for $p = 5, 13$ and a quadratic Dirichlet character ψ of conductor p. Since $\dim M_2(p) = \dim E_2(p) + \dim S_2(p)$ and $\dim M_2(p,\psi) = \dim E_2(p,\psi) + \dim S_2(p,\psi)$, we compute $\dim E_2(p)$, $\dim S_2(p)$, $\dim E_2(p,\psi)$ and $\dim S_2(p,\psi)$.

Proposition A.1. *Let p be a prime with $p \equiv 1 \pmod 4$. We have $\dim E_2(p) = 1$ for all p and $\dim S_2(p) = 0$ for $p = 5$ and 13 while $\dim S_2(p) \geq 1$ if $p > 13$. For a quadratic Dirichlet character of conductor p, we have $\dim E_2(p,\psi) = 2$ for all p and $\dim S_2(p,\psi) = 0$ for $p = 5$ and 13 while $\dim S_2(p,\psi) \geq 1$ if $p > 13$.*

Proof. Using the dimension formula of modular forms for $\Gamma_0(p)$ (see [17]), we have

$$\begin{aligned}
\dim E_2(p) &= c_0(p) - 1 \\
&= \sum_{d|p} \varphi\left(\gcd\left(d, \frac{p}{d}\right)\right) - 1 \\
&= \varphi(\gcd(1,p)) + \varphi(\gcd(p,1)) - 1 \\
&= \varphi(1) + \varphi(1) - 1 \\
&= 1.
\end{aligned}$$

For $S_2(p)$, we have

$$\begin{aligned}
\dim S_2(p) &= g_0(p) \\
&= 1 + \frac{\mu_0(p)}{12} - \frac{\mu_{0,2}(p)}{4} - \frac{\mu_{0,3}(p)}{3} - \frac{c_0(p)}{2} \\
&= 1 + \frac{p+1}{12} - \frac{1 + \left(\frac{-4}{p}\right)}{4} - \frac{1 + \left(\frac{-3}{p}\right)}{3} - \frac{2}{2} \\
&= 1 + \frac{p+1}{12} - \frac{2}{4} - \frac{1 + \left(\frac{3}{p}\right)}{3} - 1 \\
&= \frac{p+1}{12} - \frac{1}{2} - \frac{1 + \left(\frac{3}{p}\right)}{3} \\
&\begin{cases} = 0 & \text{if} \quad p = 5 \text{ or } 13, \\ \geq 1 & \text{if} \quad p > 13. \end{cases}
\end{aligned}$$

For $E_2(p,\psi)$, we have $\dim E_2(p,\psi) = \dim M_2(p,\psi) - \dim S_2(p,\psi)$. On the other hand,

$$\dim S_0(p,\psi) - \dim M_2(p,\psi) = \frac{-1}{12}\mu_0(p) - \frac{1}{2}\lambda(p,p,1) + \gamma_4(0)\sum_{x\in A_4(p)}\psi(x) + \gamma_3(0)\sum_{x\in A_3(p)}\psi(x)$$

$$-\dim M_2(p,\psi) = \frac{-(p+1)}{12} - 1 + \frac{1}{4}\sum_{x\in A_4(p)}\psi(x) + \frac{1}{3}\sum_{x\in A_3(p)}\psi(x)$$

$$\dim M_2(p,\psi) = \frac{(p+1)}{12} + 1 - \frac{1}{4}\sum_{x\in A_4(p)}\psi(x) - \frac{1}{3}\sum_{x\in A_3(p)}\psi(x).$$

We also have

$$\dim S_2(p,\psi) - \dim M_0(p,\psi) = \frac{1}{12}(p+1) - 1 - \frac{1}{4}\sum_{x\in A_4(p)}\psi(x) - \frac{1}{3}\sum_{x\in A_3(p)}\psi(x)$$

$$\dim S_2(p,\psi) = \frac{1}{12}(p+1) - 1 - \frac{1}{4}\sum_{x\in A_4(p)}\psi(x) - \frac{1}{3}\sum_{x\in A_3(p)}\psi(x).$$

Thus, $\dim E_2(p,\psi) = \dim M_2(p,\psi) - \dim S_2(p,\psi) = 2$.

We also see that

$$\dim S_2(p,\psi)\begin{cases} = 0 & \text{if} \quad p = 5 \text{ or } 13, \\ \geq 1 & \text{if} \quad p > 13. \end{cases}$$

□

BIBLIOGRAPHY

[1] T.M. Apostol, Introduction to analytic number theory. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[2] H. Cohen, Sums involving the values at negative integers of L-functions of quadratic characters. *Math. Ann.* , 217 (1975), no. 3, 271-285.

[3] H.Cohen, Number Theory. Vol. I. Tools and Diophantine equations. Graduate Texts in Mathematics, 239. Springer, New York, 2007.

[4] H. Cohen, Number Theory. Vol. II. Analytic and Modern Tools, Graduate texts in Mathematics, 240. Springer, New York, 2007.

[5] F. Diamond and J. Shurman, A first course in modular forms. Graduate Texts in Mathematics, 228. Springer-Verlag, New York, 2005.

[6] H. M. Farkas, On an arithmetical function. Ramanujan J. 8 (2004), no. 3, 309315.

[7] B. Gross, W. Kohnen and D. Zagier, Heegner points and derivatives of L-series. II. *Math. Ann.*, 278 (1987), no. 1-4, 497-562.

[8] P. Guerzhoy and W. Raji, A modular look at Farkas' identities, The Ramanujan Journal, 19 (2009), no. 1 , pp. 19-27.

[9] M. Jameson, A problem of Zagier on quadratic polynomials and continued fractions. *Int. J. Number Theory*, 12 (2016), no. 1, 121-141.

[10] L. J. P. Kilford, Modular forms. A classical and computational introduction. Imperial College Press, London, 2008.

[11] S. Lang, Introduction to modular forms. Grundlehren der mathematicschen Wissenschaften, No. 222. Springer-Verlag, Berlin, 1989.

[12] T. Miyake, Modular Forms. Translated from the Japanese by Yoshitaka Maeda. Springer-Verlag, Berlin, 1989.

[13] K. Ono, The web of modularity: arithmetic of the coefficients of modular forms and q - series. CBMS Regional Conference Series in Mathematics, 102. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004.

[14] G. Robin, Estimation de la fonction de Tchebycheff θ sur le k-i'eme nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n. *Acta Arithmetica*, XLII:367389, 1983.

[15] G. Shimura, Correspondances modulaires et les fonctions (de courbes algebriques), J. Math. Soc. Japan 10, 1-28, 1958.

[16] G. Shimura, The special values of the zeta functions associated with cusp forms. Comm. Pure Appl. Math. 29 (1976), no. 6, 783-804.

[17] W. Stein, Modular forms, a computational approach. With an appendix by Paul E. Gunnells. Graduate Studies in Mathematics, 79. American Mathematical Society, Providence, RI, 2007.

[18] K. S. Williams, Some arithmetic convolution identities, The Ramanujan Journal, 43 (2017) no. 1, pp. 197 - 213.

[19] D. Zagier, Nombres de classes et formes modulaires de poids 3/2, C. R. Acad. Sci. Paris Sér. A-B 281 (1975), no. 21.

[20] D. Zagier, Modular forms whose Fourier coefficients involve zeta-functions of quadratic fields. Modular functions of one variable, VI (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pp. 105169. Lecture Notes in Math., Vol. 627, Springer, Berlin, 1977.

[21] D. Zagier, From quadratic functions to modular functions. In *Number Theory in Progress. Vol 2 (Zakopane-Kościelisko, 1997)* , pages 1147-1178. de Gruyter, Berlin, 1999.

[22] D. Zagier, Elliptic modular forms and their applications. The 1-2-3 of modular forms, 1103, Universitext, Springer, Berlin, 2008.