

DISTRIBUTION OF VALUES OF GAUSSIAN HYPERGEOMETRIC FUNCTIONS

SATOSHI KUMABE AND HASAN SAAD

ABSTRACT. In the 1980's, Greene defined *hypergeometric functions over finite fields* using Jacobi sums. The framework of his theory establishes that these functions possess many properties that are analogous to those of the classical hypergeometric series studied by Gauss and Kummer. These functions have played important roles in the study of Apéry-style supercongruences, the Eichler-Selberg trace formula, Galois representations, and zeta-functions of arithmetic varieties. We study the value distribution (over large finite fields) of natural families of these functions. For the ${}_2F_1$ functions, the limiting distribution is semicircular (i.e. $SU(2)$), whereas the distribution for the ${}_3F_2$ functions is the *Batman* distribution for the traces of the real orthogonal group O_3 .

1. INTRODUCTION AND STATEMENT OF RESULTS

In the '80s, Greene [29, 30] defined *Gaussian hypergeometric functions* over finite fields using Jacobi sums. He developed the foundation of a beautiful theory where these functions possess many properties that are analogous to those of classical hypergeometric functions. These properties include transformation laws, explicit evaluations, and contiguous relations. These functions have played central roles in the study of combinatorial supercongruences [1, 3, 36, 44, 47, 48, 52, 55, 56, 57, 58, 59], Dwork hypersurfaces [9, 46], Galois representations [41, 42], L -functions of elliptic curves [6, 10, 11, 25, 40, 45, 53, 63, 66], hyperelliptic curves [7, 8], $K3$ surfaces [4, 19, 53], Calabi-Yau threefolds [2, 3, 68], the Eichler-Selberg trace formula [24, 25, 26, 27, 39, 49, 59, 61], among other topics. This body of work meshes well with the framework established by Katz [37] and Roberts and Villegas [62] on the analysis and arithmetic of “hypergeometric varieties”.

Here we initiate the study of the value distribution of Greene's functions. We first recall Greene's original definition. If A_1, A_2, \dots, A_n and B_1, B_2, \dots, B_{n-1} are multiplicative characters of the finite field \mathbb{F}_q , where $q = p^r$, then we have the Gaussian hypergeometric function

$${}_nF_{n-1} \left(\begin{matrix} A_1, & A_2, & \dots, & A_n \\ & B_1, & \dots, & B_{n-1} \end{matrix} \mid x \right)_q := \frac{q}{q-1} \sum_{\chi} \binom{A_1\chi}{\chi} \binom{A_2\chi}{B_1\chi} \cdots \binom{A_n\chi}{B_{n-1}\chi} \chi(x),$$

where the summation is over the multiplicative characters¹ of \mathbb{F}_q^\times , and where $\binom{A}{B}$ is the normalized Jacobi sum $J(A, B)$, defined by

$$(1.1) \quad \binom{A}{B} := \frac{B(-1)}{q} J(A, \overline{B}) := \frac{B(-1)}{q} \sum_{x \in \mathbb{F}_q} A(x) \overline{B}(1-x).$$

Many authors (see [30], [31], [35], [38], [53], and [63], to name a few) have made use of the mantra that Gaussian analogs of classical hypergeometric results arise when rational parameters

2000 *Mathematics Subject Classification.* 11F46, 11F11, 11G20, 11T24, 33E50.

Key words and phrases. Gaussian hypergeometric functions, Distributions, Elliptic curves.

¹For characters χ , we have that $\chi(0) := 0$.

$1/n$ are replaced with a character χ of order n (resp. a/n with χ^a). We consider those functions where the parameter characters have order 1 and 2, which always exist for \mathbb{F}_q when $q = p^r$ is odd. The simplest example of these functions are the ${}_2F_1$ -Gaussian hypergeometric functions

$$(1.2) \quad {}_2F_1(\lambda)_q := {}_2F_1 \left(\begin{matrix} \phi, & \phi \\ & \varepsilon \end{matrix} \middle| \lambda \right)_q = \frac{q}{q-1} \sum_{\chi} \binom{\phi\chi}{\chi} \binom{\phi\chi}{\chi} \chi(\lambda),$$

where $\phi(\cdot)$ is the quadratic character and ε is the trivial character of \mathbb{F}_q . As our first result, we compute the moments of these Gaussian hypergeometric functions.

Theorem 1.1. *If r and m are fixed positive integers, then as $p \rightarrow +\infty$ we have*

$$p^{r(m/2-1)} \sum_{\lambda \in \mathbb{F}_{p^r}} {}_2F_1(\lambda)_{p^r}^m = \begin{cases} o_{m,r}(1) & \text{if } m \text{ is odd} \\ \frac{(2n)!}{n!(n+1)!} + o_{m,r}(1) & \text{if } m = 2n \text{ is even.} \end{cases}$$

Remark. The non-zero moments in Theorem 1.1 (i.e. the Catalan numbers) arise [23] as the moments of traces of the Lie group $SU(2)$, the 2×2 determinant 1 unitary matrices. Namely, for even moments, we have

$$\int_{SU(2)} (\text{Tr} X)^{2n} dX = \frac{(2n)!}{n!(n+1)!},$$

where the integral is with respect to the Haar measure on $SU(2)$.

Using these moments, we determine the limiting behavior of the ${}_2F_1(\lambda)_{p^r}$ as $p \rightarrow +\infty$. We obtain the limiting distribution of the renormalized values $\sqrt{p^r} \cdot {}_2F_1(\lambda)_{p^r} \in [-2, 2]$, which we view as random variables on \mathbb{F}_{p^r} . Namely, we obtain the following result.

Corollary 1.2. *If $-2 \leq a < b \leq 2$, and r is a fixed positive integer, then*

$$\lim_{p \rightarrow \infty} \frac{|\{\lambda \in \mathbb{F}_{p^r} : \sqrt{p^r} \cdot {}_2F_1(\lambda)_{p^r} \in [a, b]\}|}{p^r} = \frac{1}{2\pi} \int_a^b \sqrt{4-t^2} dt.$$

Remark. Theorem 1.1 may be interpreted in terms of the Legendre normal form elliptic curves

$$E_\lambda^{\text{Leg}} : y^2 = x(x-1)(x-\lambda).$$

If $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$, then (see Theorem 11.10 of [54]) $q \cdot {}_2F_1(\lambda)_q = -\phi(-1) \cdot a_\lambda^{\text{Leg}}(q)$, where

$$(1.3) \quad a_\lambda^{\text{Leg}}(q) := q + 1 - |E_\lambda^{\text{Leg}}(\mathbb{F}_q)| = - \sum_{x \in \mathbb{F}_q} \phi(x(x-1)(x-\lambda)).$$

Corollary 1.2 refines (i.e. restriction to Legendre curves) a classical theorem of Birch [13] which established this distribution for all elliptic curves over finite fields. Birch's Theorem has recently been refined [15] by Bringmann, Kane, and Pujahari in another direction, where the Frobenius traces are restricted to arithmetic progressions. These distributions are renormalizations of the usual Sato-Tate distribution which was famously proved by Clozel, Harris, Shepherd-Barron and Taylor in [16]. In their (more difficult) setting, the elliptic curve is fixed and the distribution is taken over all primes p . Recent work along these lines for further abelian varieties have been obtained by Fité, Kedlaya, and Sutherland (for example, see [23]).

We also consider these questions for the ${}_3F_2$ Gaussian hypergeometric functions

$$(1.4) \quad {}_3F_2(\lambda)_q := {}_3F_2 \left(\begin{matrix} \phi, & \phi, & \phi \\ & \varepsilon, & \varepsilon \end{matrix} \middle| \lambda \right)_q = \frac{q}{q-1} \sum_{\chi} \binom{\phi\chi}{\chi} \binom{\phi\chi}{\chi} \binom{\phi\chi}{\chi} \chi(\lambda).$$

The power moments for these functions satisfy the following asymptotics.

Theorem 1.3. *If r and m are fixed positive integers, then as $p \rightarrow +\infty$ we have*

$$p^{r(m-1)} \sum_{\lambda \in \mathbb{F}_{p^r}} {}_3F_2(\lambda)_{p^r}^m = \begin{cases} o_{m,r}(1) & \text{if } m \text{ is odd} \\ \sum_{i=0}^m (-1)^i \binom{m}{i} \frac{(2i)!}{i!(i+1)!} + o_{m,r}(1) & \text{if } m \text{ is even.} \end{cases}$$

Remark. The moments in Theorem 1.3 arise [60] as moments of traces of the real orthogonal group O_3 . Namely, for even m we have

$$\int_{O_3} (\text{Tr} X)^m dX = \sum_{i=0}^m (-1)^i \binom{m}{i} \frac{(2i)!}{i!(i+1)!},$$

where the integral is with respect to the Haar measure on O_3 .

In analogy with Corollary 1.2, we obtain the limiting distribution of the renormalized values $p^r \cdot {}_3F_2(\lambda)_{p^r} \in [-3, 3]$, that we view as random variables over \mathbb{F}_{p^r} . We obtain the following result.

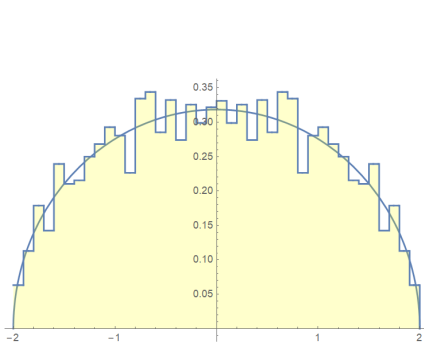
Corollary 1.4. *If $-3 \leq a < b \leq 3$, and r is a fixed positive integer, then*

$$\lim_{p \rightarrow \infty} \frac{|\{\lambda \in \mathbb{F}_{p^r} : p^r \cdot {}_3F_2(\lambda)_{p^r} \in [a, b]\}|}{p^r} = \frac{1}{4\pi} \int_a^b f(t) dt,$$

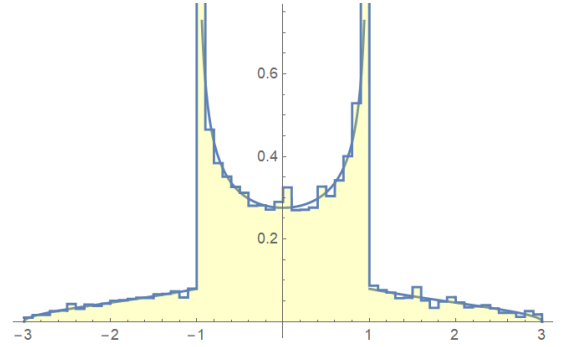
where

$$f(t) = \begin{cases} \frac{3-|t|}{\sqrt{3+2|t|-t^2}} & \text{if } 1 < |t| < 3, \\ \frac{3+t}{\sqrt{3-2t-t^2}} + \frac{3-t}{\sqrt{3+2t-t^2}} & \text{if } |t| < 1, \\ 0 & \text{otherwise.} \end{cases}$$

Example. For the prime $p = 93283$ (i.e. $r = 1$), the histograms of the values $\sqrt{p} \cdot {}_2F_1(\lambda)_p$ and $p \cdot {}_3F_2(\lambda)_p$ illustrate Corollary 1.2 (i.e. the near match with the radius 2 semicircle) and Corollary 1.4 (i.e. the near match with the Batman distribution $f(t)$).



${}_2F_1$ histogram for $p = 93283$



${}_3F_2$ histogram for $p = 93283$

Remark. Theorem 1.3 can be interpreted in terms of the $K3$ surfaces whose function fields are

$$X_\lambda : s^2 = xy(x+1)(y+1)(x+\lambda y),$$

where $\lambda \in \mathbb{F}_q \setminus \{0, -1\}$. It is known (see Theorem 11.18 of [54] and Proposition 4.1 of [4]) that

$$|X_\lambda(\mathbb{F}_q)| = 1 + q^2 + 19q + q^2 \cdot {}_3F_2(-\lambda)_q.$$

Corollary 1.4 gives the limiting Frobenius trace distribution for these $K3$ surfaces.

Remark. It is natural to consider the asymptotics for the moments of the general

$${}_nF_{n-1}(\lambda)_{p^r} := {}_nF_{n-1} \left(\begin{matrix} \phi, & \phi, & \cdots, & \phi \\ \varepsilon, & \varepsilon, & \cdots, & \varepsilon \end{matrix} \mid \lambda \right)_{p^r} = \frac{p^r}{p^r - 1} \sum_{\chi} \binom{\phi\chi}{\chi} \binom{\phi\chi}{\chi} \cdots \binom{\phi\chi}{\chi} \chi(\lambda)$$

hypergeometric functions. It would be very interesting to determine asymptotics for the moments, which in turn would lead to distributions that extend Corollaries 1.2 and 1.4. A solution to this problem in the case of the ${}_4F_3$ functions is already quite interesting.

The proofs of Theorems 1.1 and 1.3 rely on the fact that the ${}_2F_1(\lambda)_q$ and ${}_3F_2(\lambda)_q$ values arise from the arithmetic of the Legendre and Clausen elliptic curves

$$(1.5) \quad E_\lambda^{\text{Leg}} : y^2 = x(x-1)(x-\lambda) \quad \text{and} \quad E_\lambda^{\text{Cl}} : y^2 = (x-1)(x^2 + \lambda).$$

As mentioned above, the ${}_2F_1(\lambda)_q$ are renormalizations of the Frobenius traces for $E_\lambda^{\text{Leg}}/\mathbb{F}_q$. The ${}_3F_2(\lambda)_q$ (see Theorem 3.1) are related to the squares of the Frobenius traces of $E_\lambda^{\text{Cl}}/\mathbb{F}_q$. Using these arithmetic geometric connections, we reformulate the moments in terms of the moduli space of these elliptic curves. We interpret these reformulations in terms of isomorphism classes of elliptic curves with certain subgroups of \mathbb{F}_q rational points. The moments can then be given as weighted sums of Hurwitz class numbers which enumerate such isomorphism classes.

To estimate these moments, we make use of the theory of harmonic Maass forms. More precisely, these weighted sums arise in the Fourier expansions of nonholomorphic modular forms produced from the Rankin-Cohen brackets of Zagier's weight $3/2$ nonholomorphic Eisenstein series when paired with explicit theta functions. The proofs of Theorems 1.1 and 1.3 are then reduced to an application of Deligne's Theorem, which bounds the coefficients of the cuspidal components of the holomorphic projections of these nonholomorphic modular forms. The recent proof of Cohen's Conjecture by Mertens [50, 51] plays a significant role in the ${}_2F_1$ case.

This paper is organized as follows. In Section 2 we recall the fundamental facts we require about the ${}_2F_1(\lambda)_q$ functions and the arithmetic of the Legendre curves E_λ^{Leg} . In Section 3 we recall the analogous results for ${}_3F_2(\lambda)_q$ and the Clausen curves E_λ^{Cl} . In Section 4, we recall facts from the theory of harmonic Maass forms which enable us to analyze these elliptic curves in terms of weighted class number sums thanks to a theorem of Schoof. We apply these facts in Section 5 to obtain the asymptotic properties of these class number sums. In Section 6 we recall the criteria for deducing the distributions in Corollaries 1.2 and 1.4 in terms of moments. Finally, in Section 7 we conclude with the proofs of Theorems 1.1 and 1.3.

ACKNOWLEDGEMENTS

The authors thank Quanlin Chen, Eric Shen, and Drew Sutherland for comments on earlier drafts of this article. The first author thanks the Thomas Jefferson Fund and the NSF (DMS-2002265 and DMS-2055118) for their generous support, as well as the Kavli Institute grant NSF PHY-1748958. The third author is grateful for the support of a Fulbright Nehru Postdoctoral Fellowship.

2. THE ${}_2F_1(\lambda)_q$ AND THE ARITHMETIC OF E_λ^{Leg}

Here we recall important facts about the ${}_2F_1(\lambda)_q$ values. The results we require are obtained by interpreting these values in terms of the trace of Frobenius on the Legendre normal form elliptic curves E_λ^{Leg} . This connection is well known and has been observed by several authors.

Theorem 2.1 (Th. 11.10 of [54]). *If $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$ and $\text{char}(\mathbb{F}_q) \geq 5$, then*

$$q \cdot {}_2F_1(\lambda)_q = -\phi(-1)a_\lambda^{\text{Leg}}(q).$$

Remark. Theorem 2.1 is analogous to Gauss' classical hypergeometric formula for the real period $\Omega^{\text{Leg}}(\lambda)$ of E_λ^{Leg} (for example, see Chapter 9 of [33]), where for $0 < \lambda < 1$ we have

$$\pi \cdot {}_2F_1\left(\frac{1}{2} \mid \frac{1}{2} \mid \lambda\right) = \Omega^{\text{Leg}}(\lambda).$$

2.1. Facts about Legendre normal forms. As mentioned above, the proof of Theorem 1.1 relies on an arithmetic reformulation of the moments of ${}_2F_1(\lambda)_q$. By Theorem 2.1, this task requires important facts about the E_λ^{Leg} . We now recall these facts.

Proposition 2.2 (Proposition 1.7, Chapter III of [65]). *Let K be a field with $\text{char}(K) \neq 2, 3$.*

(1) *Every elliptic curve E/K is isomorphic over \overline{K} to an elliptic curve E_λ^{Leg} .*

(2) *If $\lambda \neq 0, 1$, then the j -invariant of E_λ^{Leg} is*

$$j(E_\lambda^{\text{Leg}}) = 2^8 \cdot \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

(3) *The only λ for which $j(E_\lambda^{\text{Leg}}) = 1728$ are $\lambda = 2, -1$, and $1/2$.*

(4) *The only λ for which $j(E_\lambda^{\text{Leg}}) = 0$ are $\lambda = \frac{1 \pm \sqrt{-3}}{2}$.*

(5) *For every $j \notin \{0, 1728\}$, the map $K \setminus \{0, 1\} \rightarrow j(E_\lambda^{\text{Leg}})$ is six to one. In particular, we have*

$$\left\{ \lambda, \frac{1}{\lambda}, 1 - \lambda, \frac{1}{1 - \lambda}, \frac{\lambda}{\lambda - 1}, \frac{\lambda - 1}{\lambda} \right\} \rightarrow j(E_\lambda^{\text{Leg}}).$$

Since elliptic curves defined over \mathbb{F}_q with the same j -invariant are not necessarily isomorphic over \mathbb{F}_q , we must consider the theory of twists. We only require the standard notion of a quadratic twist. If $d \in \mathbb{F}_q \setminus \{0, 1\}$, and E is given by

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

then its quadratic twist E_d is given by²

$$E_d : y^2 = dx^3 + da_2x^2 + da_4x + da_6.$$

If d is a square in \mathbb{F}_q , then E_d is isomorphic to E over \mathbb{F}_q . Moreover, if p is a prime of good reduction for E_d (and hence also E), we have that

$$(2.1) \quad q + 1 - |E(\mathbb{F}_q)| = \phi(d) (q + 1 - |E_d(\mathbb{F}_q)|).$$

The next result characterizes the quadratic twists of Legendre curves with common j -invariant.

²We note that this choice is equivalent to the usual convention where one has $E_d : dy^2 = x^3 + a_2x^2 + a_4x + a_6$.

Proposition 2.3 (Prop. 3.2 of [2]). *For $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$, the following holds.*

- (1) E_λ^{Leg} is the λ quadratic twist of $E_{1/\lambda}^{\text{Leg}}$.
- (2) E_λ^{Leg} is the -1 quadratic twist of $E_{1-\lambda}^{\text{Leg}}$.
- (3) E_λ^{Leg} is the $1-\lambda$ quadratic twist of $E_{\lambda/(\lambda-1)}^{\text{Leg}}$.
- (4) E_λ^{Leg} is the $-\lambda$ quadratic twist of $E_{(\lambda-1)/\lambda}^{\text{Leg}}$.
- (5) E_λ^{Leg} is the $\lambda-1$ quadratic twist of $E_{1/(1-\lambda)}^{\text{Leg}}$.

By Theorem 2.1, we can reformulate the moments of the ${}_2F_1$ functions as sums over Legendre normal form elliptic curves. As we shall see in the next subsection, this requires dividing these curves into isomorphism classes over \mathbb{F}_q . To this end, for $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$, we define

$$(2.2) \quad L(\lambda) := \{\beta \in \mathbb{F}_q \setminus \{0, 1\} : E_\beta^{\text{Leg}} \cong_{\mathbb{F}_q} E_\lambda^{\text{Leg}}\}.$$

The following three lemmas determine $|L(\lambda)|$. The first concerns $j \notin \{0, 1728\}$.

Lemma 2.4. *If $j(E_\lambda) \notin \{0, 1728\}$, then*

$$|L(\lambda)| = \begin{cases} 3 & \text{if } q \equiv 3 \pmod{4} \\ 6 & \text{if } q \equiv 1 \pmod{4}, \lambda \text{ and } 1-\lambda \text{ are both squares in } \mathbb{F}_q \\ 4 & \text{if } q \equiv 1 \pmod{4}, \text{ either } \lambda \text{ or } 1-\lambda \text{ is a square in } \mathbb{F}_q \\ 2 & \text{if } q \equiv 1 \pmod{4}, \text{ neither } \lambda \text{ nor } 1-\lambda \text{ is a square in } \mathbb{F}_q. \end{cases}$$

Proof. Here we consider the case where $q \equiv 3 \pmod{4}$. There are exactly two elements of $\{\lambda, 1-\lambda, -\lambda, \lambda-1\}$ that are squares. Therefore, Proposition 2.3 applies that $|L(\lambda)| = 3$. The other cases are handled *mutatis mutandis*. \square

For $j = 1728$, we have the following lemma.

Lemma 2.5. *Suppose that $E_\lambda^{\text{Leg}}/\mathbb{F}_q$ has $j(E_\lambda^{\text{Leg}}) = 1728$.*

- (1) *If $q \equiv 3 \pmod{4}$, then $a_\lambda^{\text{Leg}}(q) = 0$.*
- (2) *If $q \equiv 1 \pmod{8}$, then $L(2) = \{-1, 2, 1/2\}$.*
- (3) *If $q \equiv 5 \pmod{8}$, then $L(2) = \{-1, 2\}$ and $L(1/2) = \{1/2\}$.*

Proof. Curves with $j = 1728$ have complex multiplication by $\mathbb{Q}(i)$. There are no ideals in $\mathbb{Z}[i]$ with norm $q \equiv 3 \pmod{4}$, and so (1) follows easily (for example, see [34, Section 4]). If $q \equiv 1 \pmod{4}$, then a similar counting argument as in the proof of Lemma 2.4 gives (2) and (3). \square

For $j = 0$, we have the following lemma.

Lemma 2.6. *Suppose $E_\lambda^{\text{Leg}}/\mathbb{F}_q$ has $j(E_\lambda^{\text{Leg}}) = 0$.*

- (1) *There are no such E_λ^{Leg} when $q \equiv 2 \pmod{3}$.*
- (2) *If $q \equiv 1 \pmod{12}$, then $|L\left(\frac{1 \pm \sqrt{-3}}{2}\right)| = 2$, and $\frac{1 \pm \sqrt{-3}}{2}$ are squares in \mathbb{F}_q .*
- (3) *If $q \equiv 7 \pmod{12}$, then $|L\left(\frac{1 \pm \sqrt{-3}}{2}\right)| = 1$, and $\frac{1 \pm \sqrt{-3}}{2}$ are both not squares in \mathbb{F}_q .*

Proof. Claim (1) follows from the unsolvability of $j(E_\lambda^{\text{Leg}}) = 2^8 \cdot (\lambda^2 - \lambda + 1)^3 / \lambda^2 (\lambda - 1)^2 = 0$. The proofs of claims (2) and (3) are analogous to the proof of Lemma 2.4. \square

To obtain the desired reformulation of the power moments of the ${}_2F_1$ hypergeometric functions, we make use of the fact that $\mathbb{Z}2 \times \mathbb{Z}2 \subseteq E_\lambda^{\text{Leg}}(\mathbb{F}_q)$. Our final reformulation makes use of this

observation, combined with the fact that certain Hurwitz class numbers enumerate isomorphism classes of elliptic curves with prescribed subgroups and fixed Frobenius traces.

Lemma 2.7. *If $q \equiv 3 \pmod{4}$, and E/\mathbb{F}_q is an elliptic curve for which $\mathbb{Z}2 \times \mathbb{Z}2 \subseteq E(\mathbb{F}_q)$, then E is isomorphic to a Legendre normal form elliptic curve over \mathbb{F}_q .*

Proof. Since $\mathbb{Z}2 \times \mathbb{Z}2 \subseteq E(\mathbb{F}_q)$, E is given by

$$E : y^2 = (x - \alpha)(x - \beta)(x - \gamma),$$

where $\alpha, \beta, \gamma \in \mathbb{F}_q$. After possibly exchanging α and β , we may assume that $\beta - \alpha$ is a square. Under the transformations $y = (\beta - \alpha)^{3/2}Y$ and $x = (\beta - \alpha)X + \alpha$, $E \cong E_\lambda^{\text{Leg}}$, where $\lambda = \frac{\gamma - \alpha}{\beta - \alpha}$. \square

As the previous lemma indicates, if $q \equiv 3 \pmod{4}$, then every E/\mathbb{F}_q with $\mathbb{Z}2 \times \mathbb{Z}2 \subseteq E(\mathbb{F}_q)$ is isomorphic over \mathbb{F}_q to a Legendre normal form curve. Unfortunately, this is not the case when $q \equiv 1 \pmod{4}$, and we call those E without such isomorphic Legendre forms *inconvenient*.

Lemma 2.8. *Suppose that $q \equiv 1 \pmod{4}$ and that E/\mathbb{F}_q is inconvenient.*

- (1) *We have that $|E(\mathbb{F}_q)| \not\equiv 0 \pmod{8}$.*
- (2) *There is a $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$ and $d \in \mathbb{F}_q$, where $d \notin \mathbb{F}_q^2$, such that $\mathbb{Z}4 \times \mathbb{Z}4 \subseteq E_\lambda^{\text{Leg}}(\mathbb{F}_q)$ and $E_d \cong E_\lambda^{\text{Leg}}$ over \mathbb{F}_q .*
- (3) *The phenomenon in (2) induces a bijection between \mathbb{F}_q -isomorphism classes of inconvenient curves and those classes for which $\mathbb{Z}4 \times \mathbb{Z}4$ is a subgroup of \mathbb{F}_q -rational points.*

Proof. Let E be an elliptic curve defined by

$$E : y^2 = x(x - \alpha)(x - \beta),$$

where $\alpha, \beta, \alpha - \beta$ are non-squares in \mathbb{F}_q . The classical 2-descent lemma (for example, see Proposition X.1.4 of [65]) indicates when a rational point P is a double of another rational point, say Q . By our assumptions on α and β , we find that none of the 2-torsion points are doubles, and so we have that $|E(\mathbb{F}_q)| \not\equiv 0 \pmod{8}$. Furthermore, the α -twist E_α is

$$E_\alpha : y^2 = \alpha x(x - \alpha)(x - \beta),$$

and under the transformation $x = \alpha X, y = Y/\alpha^2$, this is equivalent to

$$E_{\beta/\alpha}^{\text{Leg}} : Y^2 = X(X - 1)(X - \beta/\alpha).$$

One then applies the 2-descent lemma again. \square

We conclude with a classification of those Legendre normal form with $\mathbb{Z}4 \times \mathbb{Z}4 \subseteq E_\lambda^{\text{Leg}}(\mathbb{F}_q)$.

Lemma 2.9. *Suppose that $q \equiv 1 \pmod{4}$ and $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$. Then we have that $\mathbb{Z}4 \times \mathbb{Z}4 \subseteq E_\lambda^{\text{Leg}}(\mathbb{F}_q)$ if and only if λ and $1 - \lambda$ are both squares in \mathbb{F}_q .*

Proof. This claim follows easily again by the 2-descent lemma. \square

2.2. Isomorphism classes of elliptic curves with prescribed subgroups. We have reformulated the moments of the ${}_2F_1$ functions as sums over isomorphism classes of elliptic curves for which $\mathbb{Z}2 \times \mathbb{Z}2 \subseteq E(\mathbb{F}_q)$. Therefore, we seek formulas for the number of such classes. Thankfully, these are known due to work of Schoof [64], and they involve Hurwitz class numbers.

To make this precise, we first recall some notation. If $-D < 0$ such that $-D \equiv 0, 1 \pmod{4}$, then denote by $\mathcal{O}(-D)$ the unique imaginary quadratic order with discriminant $-D$. Let $h(D) =$

$h(\mathcal{O}(-D))$ denote³ the order of the class group of $\mathcal{O}(-D)$ and let $\omega(D) = \omega(\mathcal{O}(-D))$ denote half the number of roots of unity in $\mathcal{O}(-D)$. Furthermore, define

$$(2.3) \quad H(D) := \sum_{\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_{\max}} h(\mathcal{O}') \quad \text{and} \quad H^*(D) := \sum_{\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_{\max}} \frac{h(\mathcal{O}')}{\omega(\mathcal{O}')},$$

where the sum is over all orders \mathcal{O}' between \mathcal{O} and the maximal order \mathcal{O}_{\max} . The following theorem of Schoof [64] gives the results we require.

Theorem 2.10 (Section 4 of [64]). *If $p \geq 5$ is prime, and $q = p^r$, then the following are true.*

(1) *If $n \geq 2$ and s is a nonzero integer for which $p|s$ and $s^2 \neq 4q$, then there are no elliptic curves E/\mathbb{F}_q with $|E(\mathbb{F}_q)| = q + 1 - s$ and $\mathbb{Z}n \times \mathbb{Z}n \subseteq E(\mathbb{F}_q)$.*

(2) *If r is even and $s = \pm 2p^{r/2}$, then the number of isomorphism classes of elliptic curves over \mathbb{F}_q with $\mathbb{Z}2 \times \mathbb{Z}2 \subseteq E(\mathbb{F}_q)$ and $|E(\mathbb{F}_q)| = q + 1 - s$ is*

$$(2.4) \quad S(p) := \frac{1}{12} \left(p + 6 - 4 \left(\frac{-3}{p} \right) - 3 \left(\frac{-4}{p} \right) \right),$$

where $\left(\frac{\cdot}{p} \right)$ is the Legendre symbol.

(3) *Suppose that n and s are integers such that $s^2 \leq 4q$, $p \nmid s$, $n^2 \mid (q + 1 - s)$, and $n \mid (q - 1)$. Then the number of isomorphism classes of elliptic curves over \mathbb{F}_q with $|E(\mathbb{F}_q)| = q + 1 - s$ and $\mathbb{Z}n \times \mathbb{Z}n \subseteq E(\mathbb{F}_q)$ is $H\left(\frac{4q-s^2}{n^2}\right)$.*

Remark. Theorem 2.10 is a compilation of various results from [64]. Namely, (1) follows from Theorem 4.2 (ii-iii) and Lemma 4.8 (i). Claim (2) follows from Theorem 4.6 and Lemma 4.8 (ii). Finally, (3) is a consequence of the proof of Theorem 4.9 (i).

Remark. The number $S(p)$ defined in (2.4) also happens to be the number of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ (for example, see Proposition 2.49 of [54]).

2.3. Formulas for ${}_2F_1$ moments. Finally, we assemble the results of the previous subsections to obtain the desired weighted class number sum expressions for the power moments.

Proposition 2.11. *Suppose that $p \geq 5$ is prime. If r and m are positive integers, then the following are true for $q = p^r$, where in each summation we have that $-2\sqrt{q} \leq s \leq 2\sqrt{q}$.*

(1) *If r is odd and m is even, then we have*

$$q^m \sum_{\lambda \in \mathbb{F}_q} {}_2F_1(\lambda)_q^m = 1 + 3 \sum_{\substack{\gcd(s,p)=1 \\ s \equiv q+1 \pmod{4}}} H^*\left(\frac{4q-s^2}{4}\right) s^m.$$

(2) *If r and m are both even, then there is a rational number $C(q) \in [0, 6]$ for which*

$$q^m \sum_{\lambda \in \mathbb{F}_q} {}_2F_1(\lambda)_q^m = 1 + C(q)S(p) \cdot q^{m/2} + 3 \sum_{\substack{\gcd(s,p)=1 \\ s \equiv q+1 \pmod{4}}} H^*\left(\frac{4q-s^2}{4}\right) s^m.$$

(3) *If $q \equiv 3 \pmod{4}$ and m is odd, then we have $q^m \sum_{\lambda \in \mathbb{F}_q} {}_2F_1(\lambda)_q^m = 1$.*

³We note that $H(D) = H^*(D) = h(D) = 0$ whenever $-D$ is neither zero nor a negative discriminant.

(4) If $q \equiv 1 \pmod{4}$ and m is odd, then there is a rational number $D(q) \in [-6, 6]$ for which

$$q^m \sum_{\lambda \in \mathbb{F}_q} {}_2F_1(\lambda)_q^m = -1 - 2 \sum_{\substack{\gcd(s,p)=1 \\ s \equiv q+1 \pmod{8}}} H^* \left(\frac{4q-s^2}{4} \right) s^m - 4 \sum_{\substack{\gcd(s,p)=1 \\ s \equiv q+1 \pmod{16}}} H^* \left(\frac{4q-s^2}{16} \right) s^m - D(q) S(p) q^{m/2}.$$

Remark. The rational number $C(q)$ is the average number of Legendre form curves in an \mathbb{F}_q -isomorphism class with $a^{\text{Leg}}(q)_\lambda = \pm 2 \cdot p^{r/2}$. Similarly, $D(q)$ is the average number of such curves in an isomorphism class with $a_\lambda^{\text{Leg}}(q) = 2p^{r/2}$ minus the average number with $a_\lambda^{\text{Leg}}(q) = -2p^{r/2}$.

Proof. We first prove (3) as it is a triviality. By Theorem 4.4 of [30], if $q \equiv 3 \pmod{4}$ and $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$, then ${}_2F_1(\lambda)_q = -{}_2F_1(1-\lambda)_q$. Therefore, claim (3) follows from the resulting cancellation, combined with the fact that ${}_2F_1(1)_q = 1/q$ and ${}_2F_1(0)_q = 0$.

The proofs of claims (1), (2), and (4) are very similar. Therefore, we only prove (4) for brevity. We make use of Theorem 2.10, and Lemmas 2.4 through 2.9. Using Theorem 2.1, we rewrite the sum in terms of $-a_\lambda^{\text{Leg}}(q)$. We then decompose the sum

$$- \sum_{\lambda \in \mathbb{F}_q \setminus \{0, 1\}} a_\lambda(q)^m = - \sum_s |I(s, q)| \cdot s^m,$$

where $I(s, q) = \left\{ \lambda \in \mathbb{F}_q \setminus \{0, 1\} : a_\lambda^{\text{Leg}}(q) = s \right\}$. By Theorem 2.10 and Lemmas 2.4-2.6, and Lemma 2.9, we have

$$\begin{aligned} - \sum_{\lambda \in \mathbb{F}_q \setminus \{0, 1\}} a_q(\lambda)^m &= -4 \sum_{\substack{\gcd(s,p)=1 \\ s \equiv q+1 \pmod{8}}} \left[H^* \left(\frac{4q-s^2}{4} \right) - H^* \left(\frac{4q-s^2}{16} \right) \right] s^m \\ &\quad - 2 \sum_{\substack{\gcd(s,p)=1 \\ s \not\equiv q+1 \pmod{8}}} H^* \left(\frac{4q-s^2}{4} \right) s^m - 6 \sum_{\substack{\gcd(s,p)=1 \\ s \equiv q+1 \pmod{16}}} H^* \left(\frac{4q-s^2}{16} \right) s^m \\ &\quad - |I(2q^{1/2}, q)| \cdot 2q^{m/2} - |I(-2q^{1/2}, q)| \cdot (-2q^{m/2}) + E(q, m), \end{aligned}$$

where $E(q, m)$ is the sum over equivalence classes which do not contain a Legendre normal form. However, by Lemma 2.8, we see that

$$E(q, m) = 2 \sum_{\substack{\gcd(s,p)=1 \\ -s \equiv q+1 \pmod{16}}} H^* \left(\frac{4q-s^2}{16} \right) s^m = 2 \sum_{\substack{\gcd(s,p)=1 \\ s \equiv q+1 \pmod{16}}} H^* \left(\frac{4q-s^2}{16} \right) (-s)^m.$$

The result follows by considering congruence conditions and the fact that m is odd. \square

3. THE ${}_3F_2(\lambda)_q$ AND THE ARITHMETIC OF E_λ^{Cl}

Here we recall important facts about the ${}_3F_2(\lambda)_q$ values, which are related to the squares of the trace of Frobenius for the Clausen elliptic curves E_λ^{Cl} .

Theorem 3.1 (Th. 5 of [53]). *If $\lambda \in \mathbb{F}_q \setminus \{0, -1\}$, $\text{char}(\mathbb{F}_q) \geq 5$ and $a_\lambda^{\text{Cl}}(q) := q + 1 - |E_\lambda^{\text{Cl}}(\mathbb{F}_q)|$, then we have*

$$q + q^2 \phi(\lambda + 1) \cdot {}_3F_2 \left(\frac{\lambda}{\lambda + 1} \right)_q = a_\lambda^{\text{Cl}}(q)^2.$$

Remark. Theorem 3.1 has a counterpart in terms of classical hypergeometric functions. For $0 < \lambda < 1$, if $\Omega^{\text{Cl}}(\lambda)$ is the real period of E_λ^{Cl} , then McCarthy [43] proved that

$${}_3F_2 \left(\frac{1}{2} \quad \frac{1}{2} \quad \frac{1}{2} \mid \frac{\lambda}{\lambda + 1} \right) = \frac{\sqrt{1 + \lambda}}{\pi^2} \cdot \Omega^{\text{Cl}}(\lambda)^2.$$

3.1. Certain moments of traces of Frobenius of the Clausen elliptic curves. The goal of this subsection is to obtain two types of power moments for the Clausen curves. To this end, we first fix some notation. We let \mathcal{C} denote a generic isomorphism class of elliptic curves over \mathbb{F}_q , where throughout $p \geq 5$ is prime and $q = p^r$, where r is a fixed positive integer. We let \mathcal{I}_q denote the set of all isomorphism classes of elliptic curves over \mathbb{F}_q , and define

$$(3.1) \quad I(s, q) := \{ \mathcal{C} \in \mathcal{I}_q : \forall E \in \mathcal{C} \text{ we have } |E(\mathbb{F}_q)| = q + 1 \pm s \},$$

$$(3.2) \quad I_2(s, q) := \{ \mathcal{C} \in I(s, q) : \forall E \in \mathcal{C} \text{ we have } E(\mathbb{F}_q)[2] \cong \mathbb{Z}2 \times \mathbb{Z}2 \},$$

where $0 < s \leq 2\sqrt{q}$ is even. We recall that the size of $I(s, q)$ is given by Theorem 2.10 as

$$|I(s, q)| = \begin{cases} 2H(4q - s^2) & \text{if } p \nmid s \\ 2 \cdot S(p) & \text{if } s^2 = 4q \text{ and } r \text{ is even} \\ 0 & \text{otherwise,} \end{cases}$$

where $S(p)$ is given by (2.4).

For even $0 < s \leq 2\sqrt{q}$, we let

$$(3.3) \quad L(s, q) = \{ \lambda \in \mathbb{F}_q \setminus \{0, -1\} : a_\lambda^{\text{Cl}}(q) = \pm s \}.$$

The following proposition about most isomorphism classes with nonzero even traces of Frobenius will simplify our later calculations.

Proposition 3.2. *If $0 < s \leq 2\sqrt{q}$ is even, $1/3, -1/9 \notin L(s, q)$, and $|E(\mathbb{F}_q)| \notin \{q + 1 \pm s\}$ for any elliptic curve E/\mathbb{F}_q with $j(E) = 1728$, then the following is true.*

(1) *If n is a positive integer, then*

$$\sum_{\substack{\lambda \in \mathbb{F}_q \setminus \{0, -1\} \\ a_\lambda^{\text{Cl}}(q) = \pm s}} a_\lambda^{\text{Cl}}(q)^{2n} = s^{2n} \cdot \left(\frac{1}{2} \cdot |I(s, q)| + |I_2(s, q)| \right).$$

(2) *If n is a positive integer, then*

$$\sum_{\substack{\lambda \in \mathbb{F}_{p^r} \setminus \{0, -1\} \\ a_\lambda^{\text{Cl}}(q) = \pm s}} \phi(-\lambda) a_\lambda^{\text{Cl}}(q)^{2n} = s^{2n} \cdot \left(-\frac{1}{2} \cdot |I(s, q)| + 2 \cdot |I_2(s, q)| \right).$$

Proof. As $I(s, q)$ includes quadratic twists, we let \mathcal{C}^{tw} be the isomorphism class of quadratic twists of curves in \mathcal{C} by nonsquares in \mathbb{F}_q , which then gives $I(s, q) = \{\mathcal{C}_1, \dots, \mathcal{C}_h, \mathcal{C}_1^{\text{tw}}, \dots, \mathcal{C}_h^{\text{tw}}\}$. To study these isomorphism classes, it is convenient to then define

$$\tilde{I}(s, q) = \{ \mathcal{C}_1 \cup \mathcal{C}_1^{\text{tw}}, \dots, \mathcal{C}_h \cup \mathcal{C}_h^{\text{tw}} \} \quad \text{and} \quad \tilde{I}_2(s, q) = \{ \mathcal{C} \cup \mathcal{C}^{\text{tw}} : \mathcal{C} \in I(s, q) \}.$$

By Theorem 2.10, we can compute $|\tilde{I}(s, q)|$ and $|\tilde{I}_2(s, q)|$. Therefore, we aim to relate the cardinalities of $L(s, q)$, $\tilde{I}(s, q)$ and $\tilde{I}_2(s, q)$. To this end, we define $F : L(s, q) \rightarrow \tilde{I}(s, q)$ by $F(\lambda) := [E_\lambda^{\text{Cl}}] \cup [E_\lambda^{\text{Cl}}]^{\text{tw}}$, where $[E]$ is the \mathbb{F}_q -isomorphism class of elliptic curves containing E .

By Lemma 7.1 [24], F is surjective, unless $j(E) = 1728$, in which case F misses exactly one isomorphism class. Furthermore, by Lemma 7.2 of [24], if $1/3, -1/9 \notin L(s, q)$, then F is three-to-one if and only if $-\lambda$ is a square in \mathbb{F}_q , and is one-to-one otherwise. To see (1), we note that the above discussion gives that

$$\sum_{\substack{\lambda \in \mathbb{F}_q \setminus \{0, -1\} \\ a_\lambda^{\text{Cl}}(q) = \pm s}} a_\lambda^{\text{Cl}}(q)^{2n} = s^{2n} \cdot \left(\frac{1}{2} (|L(s, q)| - |I_2(s, q)|) + \frac{3}{2} \cdot |I_2(s, q)| \right).$$

Similarly, to obtain (2), the above discussion gives that

$$\sum_{\substack{\lambda \in \mathbb{F}_q \setminus \{0, -1\} \\ a_\lambda^{\text{Cl}}(q) = \pm s}} \phi(-\lambda) a_\lambda^{\text{Cl}}(q)^{2n} = s^{2n} \cdot \left(-\frac{1}{2} (|L(s, q)| - |I_2(s, q)|) + \frac{3}{2} \cdot |I_2(s, q)| \right).$$

These two claims clearly reduce to (1) and (2) respectively. \square

The discussion above also provides the following critical bound for $|L(s, q)|$.

Proposition 3.3. *If $0 < s \leq 2\sqrt{q}$ is even, then we have $|L(s, q)| \leq 3 \cdot \max\{H(4q - s^2), S(p), 2\}$.*

4. HARMONIC MAASS FORMS AND WEIGHTED SUMS OF FOURIER COEFFICIENTS

In this section we explain how the weighted sums of class numbers in the previous section arise naturally in the theory of harmonic Maass forms (for background, see [14]). The connection with harmonic Maass forms stems from the following well-known theorem about Zagier's weight $3/2$ nonholomorphic Eisenstein series.

Theorem 4.1 ([67]). *The function*

$$\mathcal{H}(\tau) = -\frac{1}{12} + \sum_{n=1}^{\infty} H^*(n) q_\tau^n + \frac{1}{8\pi\sqrt{y}} + \frac{1}{4\sqrt{\pi}} \sum_{n=1}^{\infty} n \Gamma(-\frac{1}{2}; 4\pi n^2 y) q^{-n^2},$$

where $\tau = x + iy \in \mathbb{H}$ and $q_\tau := e^{2\pi i \tau}$, is a weight $3/2$ harmonic Maass form with manageable growth at the cusps of $\Gamma_0(4)$.

This theorem asserts that the generating function for Hurwitz class numbers⁴ is the *holomorphic part* of the harmonic Maass form $\mathcal{H}(\tau)$. More generally (for example, see Lemma 4.3 of [14]), every weight $k \neq 1$ harmonic weak Maass form $f(\tau)$ has a Fourier expansion of the form

$$(4.1) \quad f(\tau) = f^+(\tau) + \frac{(4\pi y)^{1-k}}{k-1} \overline{c_f^-(0)} + f^-(\tau),$$

where

$$(4.2) \quad f^+(\tau) = \sum_{n=m_0}^{\infty} c_f^+(n) q_\tau^n \quad \text{and} \quad f^-(\tau) = \sum_{\substack{n=n_0 \\ n \neq 0}}^{\infty} \overline{c_f^-(n)} n^{k-1} \Gamma(1-k; 4\pi|n|y) q_\tau^{-n}.$$

⁴Here we adopt the convention that $H^*(0) := -1/12$.

Here $\Gamma(\alpha; x) := \int_{\alpha}^{\infty} e^{-t} t^{x-1} dt$ is the usual incomplete Gamma-function. The function $f^+(\tau)$ is called the *holomorphic part* of f .

The weighted sums of class numbers we require appear in formulas for the Fourier coefficients of certain families of nonholomorphic modular forms. These forms are constructed from Zagier's $\mathcal{H}(\tau)$ as a simple implementation of the Rankin-Cohen bracket operators, which are combinatorial expressions in derivatives of pairs of modular forms. This method was previously applied by Mertens [50, 51] in his proof of a deep conjecture of Cohen on the Cohen-Eisenstein series.

4.1. Combinatorial Interlude. To carry out the strategy described above, we require a framework of combinatorial identities for the degree $a - 2$ homogeneous polynomials

$$(4.3) \quad P_{a,b}(X, Y) := \sum_{j=0}^{a-2} \binom{j+b-2}{j} X^j (X+Y)^{a-j-2},$$

where $a \geq 2$ is a positive integer and b is any real number. This framework captures the non-holomorphic modular forms constructed with the Rankin-Cohen brackets. The next proposition gives a significant identity for certain complicated algebraic expressions in these polynomials.

Proposition 4.2. *If $m > n$ are positive integers, then we have*

$$2^{-2\nu-1} \binom{2\nu+1}{\nu+1} \left(m^{-\frac{1}{2}} (m^{\frac{1}{2}} - n^{\frac{1}{2}})^{2\nu+2} \right) = \sum_{\mu=0}^{\nu} \binom{\frac{1}{2}+\nu}{\nu-\mu} \binom{\frac{1}{2}+\nu}{\mu} m^{\nu-\mu} \times \left(m^{\mu-2\nu-1/2} P_{3+2\nu, \frac{1}{2}-\mu}(m-n, n) - n^{\frac{1}{2}+\mu} \right).$$

This proposition is analogous to Proposition V.2.7 of [50]. Moreover, its proof follows along the same lines. The key lemmas we require are as follows, where binomial and multinomial coefficients with non-integral arguments are defined using the Gamma-function.

Lemma 4.3. *If $\nu \geq 1$, and $j \geq 0$ are integers, then we have*

$$\sum_{\mu=0}^{\nu} \frac{(-1)^{\mu}}{\mu - j + \frac{1}{2}} \cdot \binom{4\nu - 2\mu + 1}{2\nu - \mu, \mu, 2\nu - 2\mu + 1} = 2^{4\nu+2} (-1)^j \frac{(2\nu - j + 1)! j!}{(2j)! (2\nu - 2j + 2)!}.$$

Sketch of the Proof. This claim is analogous to Lemma V.2.6 of [50], which stems from an expression of the form

$$\sum c_{\mu} = \frac{1}{-j + \frac{1}{2}} \cdot \binom{4\nu - 1}{2\nu} \cdot {}_3F_2 \left(\begin{matrix} -\nu & -j + \frac{1}{2} & -\nu + \frac{1}{2} \\ -j + \frac{3}{2} & -2\nu + \frac{1}{2} \end{matrix} \middle| 1 \right).$$

The claim is obtained by applying the same steps to the following expression with sign changes

$$\sum c_{\mu} = \frac{1}{-j + \frac{1}{2}} \cdot \binom{4\nu + 1}{2\nu} \cdot {}_3F_2 \left(\begin{matrix} -\nu & -j + \frac{1}{2} & -\nu - \frac{1}{2} \\ -j + \frac{3}{2} & -2\nu - \frac{1}{2} \end{matrix} \middle| 1 \right).$$

□

Lemma 4.4. *The following are true:*

(1) *If $\mu \leq \nu$ are nonnegative integers, then we have*

$$\binom{\nu + \frac{1}{2}}{\nu - \mu} \binom{\nu + \frac{1}{2}}{\mu} = 2^{-2\nu-1} \binom{2\nu+1}{\nu+1} \binom{2\nu+2}{2\mu+1}.$$

(2) If $0 \leq \mu \leq \nu$ and $j \geq 0$ are integers, then we have

$$\binom{2\nu - \mu + \frac{1}{2}}{2\nu + 1 - j} \binom{j - \mu - \frac{3}{2}}{j} = \frac{(-1)^{\mu+1}}{j - \mu - \frac{1}{2}} \cdot 2^{-4\nu-2} \frac{(4\nu - 2\mu + 1)!(2\mu + 1)!}{(2\nu - \mu)! \mu! j! (2\nu - j + 1)!}.$$

Sketch of Proof. To prove (1), we emulate Mertens' proof (see p. 60 of [50]) that

$$\binom{\nu + \frac{1}{2}}{\nu - \mu} \binom{\nu - \frac{1}{2}}{\mu} = 2^{-2\nu} \binom{2\nu}{\nu} \binom{2\nu + 1}{2\mu + 1}.$$

He gives explicit steps involving standard properties of the Gamma-function that transform the left-hand side into the right-hand side. To obtain (1), one applies the same steps to

$$\binom{\nu + \frac{1}{2}}{\nu - \mu} \binom{\nu + \frac{1}{2}}{\mu}.$$

To prove (2), we emulate Mertens' proof (see p. 61 of [50]) that

$$\binom{2\nu - \mu - \frac{1}{2}}{2\nu - j} \binom{j - \mu - \frac{3}{2}}{j} = \frac{(-1)^{\mu+1}}{j - \mu - \frac{1}{2}} \cdot 2^{-4\nu} \frac{(4\nu - 2\mu - 1)!(2\mu + 1)!}{(2\nu - \mu - 1)! \mu! j! (2\nu - j)!}.$$

He gives explicit steps which transform the left-hand side into the right-hand side. To obtain (2), one applies the same steps to

$$\binom{2\nu - \mu + \frac{1}{2}}{2\nu + 1 - j} \binom{j - \mu - \frac{3}{2}}{j}.$$

□

Finally, we recall an important identity for the polynomials $P_{a,b}(X, Y)$ obtained by Mertens.

Lemma 4.5 (Lemma V.1.8 of [50]). *If $b \neq 1, 2$, then*

$$(4.4) \quad P_{a,b}(X, Y) = \sum_{j=0}^{a-2} \binom{a+b-3}{a-2-j} \binom{j+b-2}{j} (X+Y)^{a-2-j} (-Y)^j.$$

Using these lemma above, we are now able to prove Proposition 4.2.

Proof of Proposition 4.2. To prove the proposition, we begin with the right-hand side of the claimed formula. To start, we absorb the powers of m by

$$\begin{aligned} & \sum_{\mu=0}^{\nu} \binom{\frac{1}{2} + \nu}{\nu - \mu} \binom{\frac{1}{2} + \nu}{\mu} m^{\nu-\mu} \times \left(m^{\mu-2\nu-\frac{1}{2}} P_{3+2\nu, \frac{1}{2}-\mu}(r, n) - n^{\frac{1}{2}+\mu} \right) \\ &= \sum_{\mu=0}^{\nu} \binom{\nu + \frac{1}{2}}{\nu - \mu} \binom{\nu + \frac{1}{2}}{\mu} \left(m^{-\nu-\frac{1}{2}} P_{3+2\nu, \frac{1}{2}-\mu}(r, n) - n^{\frac{1}{2}+\mu} m^{\nu-\mu} \right). \end{aligned}$$

By combining Lemma 4.4 (1) with Lemma 4.5, one obtains

$$= 2^{-2\nu-1} \binom{2\nu+2}{\nu+1} \left(\sum_{\mu=0}^{\nu} \sum_{j=0}^{2\nu+1} m^{\nu-j+\frac{1}{2}} \binom{2\nu-\mu+\frac{1}{2}}{2\nu+1-j} \binom{j-\mu-\frac{3}{2}}{j} (-n)^j - \sum_{\mu=0}^{\nu} \binom{2\nu+2}{2\mu+1} n^{\frac{1}{2}+\mu} m^{\nu-\mu} \right).$$

By the Binomial Theorem, we note that the left-hand side of the claim is

$$m^{-\frac{1}{2}}(m^{\frac{1}{2}} - n^{\frac{1}{2}})^{2\nu+2} = \sum_{\mu=0}^{\nu+1} \binom{2\nu+2}{2\mu} m^{\nu-\mu+\frac{1}{2}} n^{\mu} - \sum_{\mu=0}^{\nu} \binom{2\nu+2}{2\mu+1} n^{\mu+\frac{1}{2}} m^{\nu-\mu}.$$

Therefore, it suffices to show that

$$\sum_{\mu=0}^{\nu} \sum_{j=0}^{2\nu+1} m^{\nu-j+\frac{1}{2}} \binom{2\nu-\mu+\frac{1}{2}}{2\nu+1-j} \binom{j-\mu-\frac{3}{2}}{j} (-n)^j = \sum_{\mu=0}^{\nu} \binom{2\nu+2}{2\mu} m^{\nu-\mu+\frac{1}{2}} n^{\mu}.$$

Lemma 4.4 (2), followed by an application Lemma 4.3, implies this equality. \square

4.2. Families of modular forms obtained from Rankin-Cohen brackets. As alluded to earlier, the weighted sums of class numbers we require arise in formulas for the coefficients of certain families of non-holomorphic modular forms. These families are obtained from Zagier's $\mathcal{H}(\tau)$ by making use of Rankin-Cohen brackets. In this section we recall several important facts about the nonholomorphic modular forms obtained by this method, along with their holomorphic modular form images under the process of holomorphic projection.

To make this precise, let f and g be smooth functions defined on the upper-half of the complex plane \mathbb{H} , and let $k, l \in \mathbb{R}_{>0}$ and $\nu \in \mathbb{N}_0$. The ν th *Rankin-Cohen bracket* of f and g is

$$(4.5) \quad [f, g]_{\nu} := \frac{1}{(2\pi i)^{\nu}} \sum_{r+s=\nu} (-1)^r \binom{k+\nu-1}{s} \binom{l+\nu-1}{r} \frac{d^r}{d\tau^r} f \cdot \frac{d^s}{d\tau^s} g.$$

As the next proposition illustrates, these operators preserve modularity.

Proposition 4.6 (Th. 7.1 of [17]). *Let f and g be (not necessarily holomorphic) modular forms of weights k and l , respectively on a congruence subgroup Γ . Then the following are true.*

- (1) *We have that $[f, g]_{\nu}$ is modular of weight $k + l + 2\nu$ on Γ .*
- (2) *If $\gamma \in SL_2(\mathbb{R})$, then under the usual modular slash operator we have*

$$[f|_k \gamma, g|_l \gamma]_{\nu} = ([f, g]_{\nu})|_{k+l+2\nu} \gamma.$$

Remark. Proposition 4.6 (2) is important for studying the behavior of Rankin-Cohen brackets at cusps. It shows that if f and g are smooth functions that do not blow up at any cusp, and $[f, g]_{\nu}$ vanishes at the cusp $i\infty$, then it vanishes at all other cusps for $\nu > 0$.

By Proposition 4.6, we have a procedure for producing many nonholomorphic modular forms from derivatives of a pair of seed forms f and g . We shall study forms that arise in this way from $f(\tau) := \mathcal{H}(\tau)$ and certain univariate theta functions for $g(\tau)$. To prove our results, we make use of canonical holomorphic modular forms that have coefficients with the same asymptotic properties as $[f, g]_{\nu}$. These forms are obtained by the method of holomorphic projection.

To make this precise, suppose $f : \mathbb{H} \rightarrow \mathbb{C}$ is a (not necessarily holomorphic) modular form of weight $k \geq 2$ on a congruence subgroup Γ with Fourier expansion

$$f(\tau) = \sum_{n \in \mathbb{Z}} c_f(n, y) q_{\tau}^n,$$

where $\tau = x + iy$. Let $\{\kappa_1, \dots, \kappa_M\}$ be the cusps of Γ , where $\kappa_1 := i\infty$. Moreover, for each j let $\gamma_j \in SL_2(\mathbb{Z})$ satisfy $\gamma_j \kappa_j = i\infty$. Then suppose the following are true.

(1) There is an $\varepsilon > 0$ and a constant $c_0^{(j)} \in \mathbb{C}$ for which

$$f(\gamma_j^{-1}w) \left(\frac{d\tau}{dw} \right)^{k/2} = c_0^{(j)} + O(\text{Im}(w))^{-\varepsilon},$$

for all $j = 1, \dots, M$ and $w = \gamma_j \tau$.

(2) For all $n > 0$, we have that $c_f(n, y) = O(y^{2-k})$ as $y \rightarrow 0$. Then, the *holomorphic projection* of f is defined by

$$(4.6) \quad (\pi_{\text{hol}} f)(\tau) := c_0 + \sum_{n=1}^{\infty} c(n) q_{\tau}^n,$$

where $c_0 = c_0^{(1)}$ and for $n \geq 1$

$$c(n) = \frac{(4\pi n)^{k-1}}{(k-2)!} \int_0^{\infty} c_f(n, y) e^{-4\pi n y} y^{k-2} dy.$$

The following proposition explains the important role of the projection operator.

Proposition 4.7 (Prop. 10.2 of [14]). *Assuming the hypotheses above, if $k > 2$ (resp. $k = 2$), then $\pi_{\text{hol}}(f)$ is a weight k holomorphic modular form (resp. weight 2 quasimodular form) on Γ .*

Turning to the setting we consider, suppose that f is a harmonic Maass form of weight $k \in \frac{1}{2}\mathbb{Z}$ on $\Gamma_0(N)$ with manageable growth at the cusps, and that g is a holomorphic modular form of weight l on $\Gamma_0(N)$. Moreover, suppose that $[f, g]_{\nu}$ satisfies the hypothesis in the definition of holomorphic projection. By additivity, the holomorphic modular form obtained by Proposition 4.7 has the following convenient decomposition

$$(4.7) \quad \pi_{\text{hol}}([f, g]_{\nu}) = [f^+, g]_{\nu} + \frac{(4\pi)^{1-k}}{k-1} \overline{c_f^-(0)} \pi_{\text{hol}}([y^{1-k}, g]_{\nu}) + \pi_{\text{hol}}([f^-, g]_{\nu}).$$

For our applications, the weighted class number sums will arise from the first summand $[f^+, g]_{\nu}$ of (4.7), when $g(\tau)$ is a univariate theta function, and $f(\tau) = \mathcal{H}(\tau)$. This term $[\mathcal{H}, g]_{\nu}$ clearly involves weighted sums of class numbers via Theorem 4.1.

The other two summands in (4.7) must be bounded for our applications. The next lemma offers a closed formula for the Fourier expansion of the middle term.

Lemma 4.8 (Lemma V.1.4 of [50]). *Assuming the hypotheses above, if $g(\tau)$ has Fourier series $g(\tau) = \sum_{n=0}^{\infty} a_g(n) q_{\tau}^n$, then we have*

$$\frac{(4\pi)^{1-k}}{k-1} \pi_{\text{hol}}([y^{1-k}, g]_{\nu}) = \kappa(k, l, \nu) \cdot \sum_{n=0}^{\infty} n^{k+\nu-1} a_g(n) q_{\tau}^n,$$

where

$$\kappa(k, l, \nu) := \frac{1}{(k+l+2\nu-2)!(k-1)} \sum_{\mu=0}^{\nu} \left(\frac{\Gamma(2-k)\Gamma(l+2\nu-\mu)}{\Gamma(2-k-\mu)} \binom{k+\nu-1}{\nu-\mu} \binom{l+\nu-1}{\mu} \right).$$

Finally, the last term in (4.7) can be bounded thanks to the following theorem of Mertens that offers a closed formula in terms of the Fourier coefficients of f and g .

Theorem 4.9 (Th. V.1.5 of [50]). *If $c_f^-(n)$ and $a_g(n)$ are bounded polynomially, then we have $\pi_{hol}([f^-, g]_\nu = \sum_{r=1}^{\infty} b(r)q_\tau^r$, where*

$$b(r) = -\Gamma(1-k) \sum_{m-n=r} a_g(m) \overline{c_f^-(n)} \sum_{\mu=0}^{\nu} \binom{k+\nu-1}{\nu-\mu} \binom{l+\nu-1}{\mu} m^{\nu-\mu} \\ \times (m^{\mu-2\nu-l+1} P_{k+l+2\nu, 2-k-\mu}(r, n) - n^{k+\mu-1}),$$

where the sum runs over positive integers m and n .

Remark. We shall apply Proposition 4.2, the main objective of the previous subsection, to the formulas in the theorem above. This application yields convenient formulas for the Fourier expansions of important modular forms (for example, see (4.2)) constructed in the next section.

5. BOUNDS FOR WEIGHTED SUMS OF CLASS NUMBERS

Here we assemble the required asymptotics for the weighted sums of class numbers that lead to the proofs of Theorems 1.1 and 1.3. The proofs of these asymptotics rely on standard bounds for class numbers and coefficients of cusp forms, and the results of Section 4 on the holomorphic projection of those nonholomorphic modular forms arising from the Rankin-Cohen bracket of Zagier's $\mathcal{H}(\tau)$ function with certain univariate theta functions.

5.1. Some Standard Bounds. Here we recall some simple class numbers bounds, and the celebrated theorem of Deligne which bounds the coefficients of integer weight cusp forms.

Lemma 5.1. *The following are true.*

- (1) *If $-D < 0$ is a discriminant, then we have $H^*(D) \leq \sqrt{D}(\log D + 2)/\pi$.*
- (2) *For fixed positive integers r and m , as the primes $p \rightarrow +\infty$, we have*

$$\sum_{s \in \Omega_{p^r}} H^* \left(\frac{4p^r - s^2}{4} \right) s^m = o_{m,r}(p^{r(m/2+1)}),$$

where $\Omega_{p^r} := \{s \in [-2\sqrt{p^r}, 2\sqrt{p^r}] : p \mid s \text{ and } s \equiv p^r + 1 \pmod{4}\}$.

Proof. Claim (1) is Lemma 2.2 of [32]. To prove (2), we note that at most $2p^{r/2-1}$ nonzero integers s such that $s^2 \leq 4p^r$ and $p \mid s$. Therefore, we have the following trivial bound

$$\sum_{s \in \Omega_{p^r}} H^* \left(\frac{4p^r - s^2}{4} \right) s^m \leq 2p^{r/2-1} (2p^{r/2})^m \cdot \max \left\{ H^* \left(\frac{4p^r - s^2}{4} \right) \right\}.$$

Claim (2) follows immediately now from (1). □

The following celebrated theorem of Deligne, which bounds the coefficients of integer weight cusp forms, shall also play a key role in our subsequent work.

Theorem 5.2 (Remark 9.3.15 of [18]). *If $f = \sum_{n \geq 1} a(n)q_\tau^n$ is a cusp form of integer weight k on a congruence subgroup, then for all $\varepsilon > 0$ we have $a(n) = O_\varepsilon(n^{(k-1)/2+\varepsilon})$.*

5.2. Weighted sums of class numbers required for Theorem 1.1. We now derive the asymptotic formulas which are crucial for the proof of Theorem 1.1.

5.2.1. *Even moments.* We begin by recalling the famous classical result of Eichler.

Theorem 5.3 (Eichler [20, 21]). *If N is odd, then*

$$\sum_{-\sqrt{N} \leq s \leq \sqrt{N}} H^*(N - s^2) = -\lambda_1(N) + \frac{1}{3}\sigma_1(N),$$

where $\sigma_1(N) := \sum_{d|N} d$, and $\lambda_1(N) := \frac{1}{2} \sum_{d|N} \min(d, \frac{N}{d})$.

From Eichler's identity, if $q = p^r$, where p is an odd prime, then we find that

$$3 \sum_{-\sqrt{q} \leq s \leq \sqrt{q}} H^*(q - s^2) = q + o_r(q)$$

This conclusion is the $n = 0$ case of the following general family of asymptotics.

Lemma 5.4. *If n is a nonnegative integer, then*

$$3 \sum_{s \equiv q+1 \pmod{4}} H^*\left(\frac{4q - s^2}{4}\right) s^{2n} = \frac{(2n)!}{n!(n+1)!} \cdot q^{n+1} + o_n(q^{n+1}).$$

Proof. Since $H^*(D) = 0$ for $D \equiv 1, 2 \pmod{4}$, we have

$$\sum_{s \equiv q+1 \pmod{4}} H^*\left(\frac{4q - s^2}{4}\right) s^{2n} = 2^{2n} \sum_s s^{2n} H^*(q - s^2).$$

Mertens recently proved Cohen's Conjecture (see Conjecture I.2.1 of [50] and [17]) which constructs an infinite sequence of cusp forms from Hurwitz class numbers. Namely, if n is a positive integer, then he proves (see Theorem 1 of [51]) that the coefficient of X^{2n} in

$$\sum_{l \text{ odd}} \left[\sum_{s \in \mathbb{Z}} \frac{H^*(l - s^2)}{1 - 2sX + lX^2} + \sum_{k=0}^{\infty} \lambda_{2k+1}(l) X^{2k} \right] q_\tau^l$$

is a cusp form of weight $2n+2$ on $\Gamma_0(4)$, where $\lambda_{2k+1}(l) := \frac{1}{2} \sum_{d|l} \min(d, \frac{l}{d})^{2k+1}$. On the other hand,

Lemma 7.5 of [17] establishes that the coefficient of X^{2n} is the Fourier series

$$\sum_{l \text{ odd}} q_\tau^l \left[\sum_{0 \leq t \leq n} (-1)^t \frac{(2n-t)! l^t}{t!(2n-2t)!} \sum_s H^*(l - s^2) (2s)^{n-2t} + \lambda_{2n+1}(l) \right].$$

We now prove the lemma by mathematical induction on n . Thanks to Eichler's Theorem 5.3, the claim holds for $n = 0$. Now, suppose that the lemma is true for $n' < n$. It is clear that $\lambda_{2n+1}(q) = O(q^{n+3/4}) = o(q^{n+1})$ as $q \rightarrow \infty$. Therefore, Deligne's Theorem 5.2 implies that

$$(5.1) \quad \sum_{1 \leq t \leq n} (-1)^t \frac{(2n-t)! q^t}{t!(2n-2t)!} \sum_s H^*(q - s^2) (2s)^{2n-2t} + \sum_s H^*(q - s^2) (2s)^{2n} = o_n(q^{n+1}).$$

By the induction hypothesis, replacing $\sum_s H^*(q - s^2)(2s)^{2n-2t}$ by $\frac{(2n-2t)!}{3(n-t)!(n-t+1)!} q^{n-t+1}$ contributes $o_n(q^{n-t+1})$. Therefore, we have

$$\begin{aligned} 3 \sum_s H^*(q - s^2)(2s)^{2n} &= - \sum_{1 \leq t \leq n} (-1)^t \frac{(2n-t)!}{t!(n-t)!(n+1-t)!} \cdot q^{n+1} + o_n(q^{n+1}) \\ &= \frac{(2n)!}{n!(n+1)!} q^{n+1} - \sum_{0 \leq t \leq n} (-1)^t \frac{(2n-t)!}{t!(n-t)!(n+1-t)!} \cdot q^{n+1} + o_n(q^{n+1}). \end{aligned}$$

Cohen computed $(1-t)^{l+1} \cdot (1-t)^{-l-1}$ in two ways, and proved (see p. 284 of [17]) that

$$\sum_{0 \leq t \leq n} (-1)^t \frac{(2n-t)!}{t!(n-t)!(n+1-t)!} = 0,$$

thereby completing the proof. □

5.2.2. Odd moments. The following lemma provides an asymptotic formula for a modified version of the weighted sum of Hurwitz class numbers which appears in Proposition 2.11 (4).

Lemma 5.5. *If m is a positive odd integer, then the following are true.*

(1) *As $q \rightarrow \infty$ with $q \equiv 1 \pmod{4}$, we have*

$$\sum_{s \equiv q+1 \pmod{8}} H^*\left(\frac{4q-s^2}{4}\right) s^m = o_m(q^{m/2+1}).$$

(2) *As $q \rightarrow \infty$ with $q \equiv 1 \pmod{4}$, we have*

$$\sum_{s \equiv q+1 \pmod{16}} H^*\left(\frac{4q-s^2}{16}\right) s^m = o_m(q^{m/2+1}).$$

Proof. Here we prove case (1) when $q \equiv 1, 5 \pmod{8}$. The proof of (2) is completely analogous and shall be left to the reader. To this end, let $g(\tau) = \eta(8\tau)^3$, where $\eta(\tau) = q_\tau^{1/24} \prod_{n=1}^{\infty} (1 - q_\tau^n)$ is the Dedekind eta-function. It is the weight $3/2$ cuspidal theta function on $\Gamma_0(64)$ for the Dirichlet character $\chi_{-4} := \left(\frac{-4}{\bullet}\right)$. By Theorem 4.1 and Proposition 4.7, we have that $\pi_{\text{hol}}(\mathcal{H} \cdot g)$ is a holomorphic modular form of weight 3 on $\Gamma_0(64)$ and Nebentypus character χ_{-4} . Moreover, since \mathcal{H} has manageable growth at cusps and g is a cusp form, Proposition 4.6 (2) implies that $\pi_{\text{hol}}(\mathcal{H} \cdot g)$ is a cusp form. Thanks to Proposition 4.2, Lemma 4.8, and Theorem 4.9, its Fourier expansion is

$$\begin{aligned} (5.2) \quad \sum_{n=1}^{\infty} \left(\sum_{s \equiv 1 \pmod{4}} H^*(n - s^2) s \right) q_\tau^n &+ \frac{1}{4} \sum_{n=1}^{\infty} \left(\sum_{\substack{t^2 - l^2 = n \\ t, l \geq 1}} \chi_{-4}(t) \cdot (t-l)^2 \right) q_\tau^n \\ &+ \frac{1}{8} \sum_{n=0}^{\infty} \chi_{-4}(n) \cdot n^2 q_\tau^{n^2}. \end{aligned}$$

Since we have $\sum_{\substack{t^2-l^2=n \\ t,l \geq 1}} (t-l)^2 \leq n^{\frac{1}{2}} \cdot d(n)$, where $d(n)$ is the divisor function, it is clear that $\sum_{\substack{t^2-l^2=n \\ t,l \geq 1}} (t-l)^2 = o(n^{3/2})$. Claim (1) with $m = 1$ follows from Theorem 5.2 as we have

$$\sum_{s \equiv 2 \pmod{8}} H^* \left(\frac{4q - s^2}{4} \right) s^m = \sum_{s \equiv 1 \pmod{4}} H^*(q - s^2) (2s)^m.$$

We proceed by induction. Suppose that it is true for $m' < m$. If $\nu = (m-1)/2$, then it is easy to verify that

$$[\mathcal{H}^+, g]_\nu = \sum_{n=0}^{\infty} \left(\sum_{j=0}^{\nu} (-1)^j \binom{\nu + \frac{1}{2}}{j} \binom{\nu + \frac{1}{2}}{\nu - j} \sum_{s \equiv 1 \pmod{4}} s^{2\nu-2j+1} (n-s^2)^j H^*(n-s^2) \right) q_\tau^n.$$

Therefore, as above, we have that

$$\begin{aligned} & \sum_{n=0}^{\infty} \left(\sum_{j=0}^{\nu} (-1)^j \binom{\nu + \frac{1}{2}}{j} \binom{\nu + \frac{1}{2}}{\nu - j} \sum_{s \equiv 1 \pmod{4}} s^{2\nu-2j+1} (n-s^2)^j H^*(n-s^2) \right) q_\tau^n \\ & + 2^{-2\nu-2} \binom{2\nu+1}{\nu+1} \sum_{n=1}^{\infty} \left(\sum_{\substack{t^2-l^2=n \\ t,l \geq 1}} \chi(t)(t-l)^{2\nu+2} \right) q_\tau^n + \frac{\kappa}{8\sqrt{\pi}} \sum_{n=0}^{\infty} \chi(n) n^{2\nu+2} q_\tau^{n^2}, \end{aligned}$$

where $\kappa = \kappa(3/2, 3/2, \nu)$ is as in Lemma 4.8, is a cusp form of weight $2\nu+3$ on $\Gamma_0(64)$ and Nebentypus character χ_{-4} . The proof follows similarly as in the case $m = 1$ with an induction argument for the first sum. \square

5.3. Weighted sums of class numbers required for Theorem 1.3. We state an asymptotic formula for weighted sums of class numbers which are important to prove Theorem 1.3. For brevity, we sketch the proof as it follows the same arguments from the previous section.

Lemma 5.6. *If n is a nonnegative integer, then as $q \rightarrow +\infty$ we have*

$$\sum_{s \text{ even}} H^*(4q - s^2) s^{2n} = \frac{4}{3} \cdot \frac{(2n)!}{n!(n+1)!} q^{n+1} + o_n(q^{n+1}).$$

Sketch of the proof. First, we write

$$\sum_{s \text{ even}} H^*(4q - s^2) s^{2n} = 2^{2n} \sum_s H^*(4q - 4s^2) s^{2n}.$$

To adapt the proof of Lemma 5.5, let $g(\tau) = \theta(4\tau)$, where $\theta(\tau) = \sum_{n \in \mathbb{Z}} q_\tau^{n^2} = 1 + 2q_\tau + 2q_\tau^4 + \dots$ is the usual weight $1/2$ Jacobi θ function. Then g is a modular form of weight $1/2$ on $\Gamma_0(16)$. The proof for $\nu = 0$ follows from a simple counting argument for the number of Clausen models. Then the proof by induction follows the same steps as in the proof of Lemma 5.5 when modified suitably for the weight $1/2$ univariate theta function $g(\tau) = \theta(4\tau)$. \square

6. SOME DISTRIBUTIONS

To obtain Corollaries 1.2 and 1.4, we will combine Theorem 1.1 and 1.3 with the following lemma concerning the semicircular and Batman distributions. To make this precise, we first let \mathbb{P} denote the set of primes, and fix a positive integer r . For each prime $p \in \mathbb{P}$, we have a function

$$f_p : \mathbb{F}_{p^r} \rightarrow [-1, 1].$$

In this notation, we have the following important lemma.

Lemma 6.1. *If r is a fixed positive integer, then the following are true.*

(1) *Suppose that the following asymptotics hold for every positive integer m :*

$$\sum_{\lambda \in \mathbb{F}_{p^r}} f_p(\lambda)^m = \begin{cases} o_{m,r}(1) & \text{if } m \text{ is odd} \\ \frac{(2n)!}{2^{2n}(n+1)!n!} + o_{m,r}(1) & \text{if } m = 2n \text{ is even.} \end{cases}$$

If $-1 \leq a < b \leq 1$, then

$$\lim_{p \rightarrow \infty} \frac{|\{\lambda \in \mathbb{F}_{p^r} : f_p(\lambda) \in [a, b]\}|}{p^r} = \frac{2}{\pi} \int_a^b \sqrt{1-t^2} dt.$$

(2) *Suppose that the following asymptotics hold for every positive integer m :*

$$\sum_{\lambda \in \mathbb{F}_{p^r}} f_p(\lambda)^m = \begin{cases} o_{m,r}(1) & \text{if } m \text{ is odd} \\ \sum_{i=0}^m (-1)^i \binom{m}{i} \frac{(2i)!}{3^m i!(i+1)!} + o_{m,r}(1) & \text{if } m \text{ is even.} \end{cases}$$

If $-1 \leq a < b \leq 1$, then

$$\lim_{p \rightarrow \infty} \frac{|\{\lambda \in \mathbb{F}_{p^r} : f_p(\lambda) \in [a, b]\}|}{p^r} = \frac{3}{4\pi} \int_a^b f(t) dt,$$

where

$$f(t) = \begin{cases} \frac{3-3|t|}{\sqrt{3+6|t|-9t^2}} & \text{if } \frac{1}{3} < |t| < 1 \\ \frac{3+3t}{\sqrt{3-6t-9t^2}} + \frac{3-3t}{\sqrt{3+6t-9t^2}} & \text{if } |t| < \frac{1}{3} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. This result follows via a standard application of the method of moments in probability theory (for example, see Theorems 30.1 and 30.2 of [12]). We prove these two cases separately.

(1) For each $p \in \mathbb{P}$, consider the probability space $(\Omega_p, \mathcal{F}_p, \mu_p)$, where $\Omega_p = \mathbb{F}_{p^r}$, $\mathcal{F}_p = \mathcal{P}(\mathbb{F}_{p^r})$, and $\mu_p(A) = |A|/p^r$ for all $A \in \mathcal{F}_p$. For the random variable $X_p = f_p$, we have

$$\lim_{p \rightarrow \infty} E(X_p^m) = \begin{cases} 0 & \text{if } m \text{ is odd} \\ \frac{(2n)!}{2^{2n}(n+1)!n!} & \text{if } m = 2n \text{ is even.} \end{cases}$$

Furthermore, consider the probability space $(\Omega, \mathcal{F}, \mu_{ST})$, where $\Omega := [-1, 1]$, \mathcal{F} is the collection of Lebesgue-measurable subsets of Ω , and μ_{ST} is the measure $\mu_{ST}([a, b]) := \frac{2}{\pi} \int_a^b \sqrt{1-t^2} dt$.

For the random variable $X : \Omega \rightarrow [-1, 1]$, defined by $X(t) := t$, we have

$$E(X^m) = \begin{cases} 0 & \text{if } m \text{ is odd} \\ \frac{(2n)!}{2^{2n}(n+1)!n!} & \text{if } m = 2n \text{ is even.} \end{cases}$$

Since the moment-generating function has a positive radius of convergence, the distribution of X is determined by its moments, and thus X_p converges in distribution to X . Therefore, for $-1 \leq a < b \leq 1$, we have

$$\lim_{p \rightarrow \infty} \frac{|\{\lambda \in \mathbb{F}_{p^r} : f_p(\lambda) \in [a, b]\}|}{p^r} = \lim_{p \rightarrow \infty} \mu_p(\{a \leq X_p \leq b\}) = \mu_{ST}(a \leq X \leq b).$$

(2) The proof of the second case follows *mutatis mutandis*. The only change is that

$$\int_{-3}^3 f(t)t^m dt = \begin{cases} 0 & \text{if } m \text{ is odd} \\ 4\pi \sum_{i=0}^m (-1)^i \binom{m}{i} \frac{(2i)!}{i!(i+1)!} & \text{if } m \text{ is even,} \end{cases}$$

where $f(t)$ is as in Corollary 1.4. Since f is odd, it is clear that $\int_{-3}^3 f(t)t^m dt = 0$ when m is odd. By symmetry, when m is even, we have

$$\int_{-3}^3 f(t)t^m dt = 2 \int_{-1}^3 \sqrt{\frac{3-t}{1+t}} \cdot t^m dt.$$

By a simple change of variables, we see that

$$\int_{-3}^3 f(t)t^m dt = 8 \int_0^1 t^{-1/2}(1-t)^{1/2}(1-4t)^m dt.$$

Thankfully, we can express this integral in terms of the Appell hypergeometric series

$$F_1(a, b_1, b_2; c; x, y) := \sum_{k,n=0}^{\infty} \frac{(a)_{k+n}(b_1)_k(b_2)_n}{(c)_{k+n}k!n!} \cdot x^k y^n,$$

where c is not a nonnegative integer, and $(r)_n := \prod_{k=0}^{n-1} (r+k)$ for $n \geq 1$, and $(r)_0 = 1$. By a formula of Bailey (see page 77, (4) of [5]), we have

$$\int_0^1 t^u \left(1 - \frac{t}{a}\right)^v \left(1 - \frac{t}{b}\right)^w dt = \frac{1}{u+1} \cdot F_1\left(u+1, -v, -w; u+2; \frac{1}{a}, \frac{1}{b}\right).$$

By letting $u = -\frac{1}{2}$, $v = \frac{1}{2}$, $w = m$, $a = 1$, and $b = \frac{1}{4}$, we obtain⁵

$$(6.1) \quad \int_{-3}^3 f(t)t^m dt = 16 \cdot F_1\left(\frac{1}{2}, -\frac{1}{2}, -m; \frac{3}{2}; 1, 4\right).$$

To find an exact formula, we will need the classical hypergeometric series

$${}_2F_1\left(\begin{matrix} a & b \\ c \end{matrix} \middle| z\right) := \sum_{n=0}^{\infty} \frac{(a)_n(b)_n}{(c)_n} \cdot \frac{z^n}{n!},$$

where c cannot be a nonnegative integer. It is straightforward to see that

$$F_1(a, b_1, b_2; c; 1, x) = {}_2F_1\left(\begin{matrix} a & b_1 \\ c \end{matrix} \middle| 1\right) \cdot {}_2F_1\left(\begin{matrix} a & b_2 \\ c - b_1 \end{matrix} \middle| x\right).$$

⁵This series converges since $-m$ is negative integer.

Substituting this identity into (6.1), we obtain

$$(6.2) \quad \int_{-3}^3 f(t)t^m dt = 16 \cdot {}_2F_1 \left(\begin{matrix} \frac{1}{2} & -\frac{1}{2} \\ \frac{3}{2} & | 1 \end{matrix} \right) \cdot {}_2F_1 \left(\begin{matrix} \frac{1}{2} & -m \\ 2 & | 4 \end{matrix} \right).$$

Using Gauss' identity (see (1.3) of [5], and [28])

$${}_2F_1 \left(\begin{matrix} a & b \\ c & | 1 \end{matrix} \right) = \frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)},$$

where $\operatorname{Re}(c-a-b) > 0$, we find that

$$\int_{-3}^3 f(t)t^m dt = 4\pi \cdot {}_2F_1 \left(\begin{matrix} \frac{1}{2} & -m \\ 2 & | 4 \end{matrix} \right) = 4\pi \sum_{k=0}^m (-1)^k \binom{m}{k} \frac{(2k)!}{k!(k+1)!}.$$

The claim in the proposition follows by an elementary rescaling. \square

7. PROOFS OF THEOREMS 1.1 AND 1.3 AND COROLLARIES 1.2 AND 1.4

We now prove Theorems 1.1 and 1.3, and their corollaries.

Proof of Theorem 1.1. Proposition 2.11 gives a formula for the power moments of the values of the hypergeometric functions ${}_2F_1(\lambda)_q$ in terms of weighted sums of class numbers. Lemma 5.1 (2) reduces the statement to Lemmas 5.4 and 5.5, thereby concluding the proof. \square

Proof of Corollary 1.2. After rescaling, the claim follows from Theorem 1.1 and Lemma 6.1 (1). \square

Proof of Theorem 1.3. By Proposition 3.2 and Lemma 5.1 (2), we have that

$$\sum_{\lambda \in \mathbb{F}_{p^r}} a_{\lambda}^{\text{Cl}}(p^r)^{2n} = \frac{(2n)!}{n!(n+1)!} \cdot p^{rn+r} + o_n(p^{rn+r}) \quad \text{and} \quad \sum_{\lambda \in \mathbb{F}_{p^r}} \phi(-\lambda) a_{\lambda}^{\text{Cl}}(p^r)^{2n} = o_n(p^{rn+r}),$$

for all positive integers n . Since ${}_3F_2(\beta)_q = \phi(-\beta){}_3F_2(1/\beta)_q$ for all $\beta \in \mathbb{F}_q^{\times}$ (see Theorem 4.2 of [30]), Theorem 3.1 gives us that

$$\phi(\lambda+1) a_{\lambda}^{\text{Cl}}(q)^2 = \phi(\lambda+1) a_{-\lambda-1}^{\text{Cl}}(q)^2.$$

Applying the binomial theorem to the equation in Theorem 3.1 concludes the proof. \square

Proof of Corollary 1.4. After rescaling, the claim follows from Theorem 1.3 and Lemma 6.1 (2). \square

REFERENCES

- [1] S. Ahlgren, *Gaussian hypergeometric series and combinatorial congruences*, Symbolic computation, number theory, special functions, physics, and combinatorics (Gainesville, Fl., 1999), Dev. Math. **4**, Kluwer Acad. Publ., Dordrecht, 2001, 1-12.
- [2] S. Ahlgren and K. Ono, *Modularity of a certain Calabi-Yau threefold*, Montash. Math. **129** (3) (2000), 177-190.
- [3] S. Ahlgren and K. Ono, *A Gaussian hypergeometric series evaluation and Apéry number congruences*, J. Reine Angew. Math. **518** (2000), 187-212.
- [4] S. Ahlgren, K. Ono, and D. Penniston, *Zeta functions of an infinite family of K3 surfaces*, Amer. J. Math., **124** (2) (2002), 353-368.
- [5] W. Bailey, *Generalized hypergeometric series*, Cambridge Tracts in Mathematics and Mathematical Physics **32**, Cambridge Univ. Press, Cambridge, 1935.

- [6] R. Barman and G. Kalita, *Hypergeometric functions over \mathbb{F}_q and traces of Frobenius for elliptic curves*, Proc. Amer. Math. Soc. **141** (2013), 3403-3410.
- [7] R. Barman, G. Kalita and N. Saikia, *Hyperelliptic curves and values of Gaussian hypergeometric series*, Arch. Math. (Basel), **102** (2014), 345-355.
- [8] R. Barman, D. McCarthy, and N. Saikia, *Summation identities and special values of hypergeometric series in the p -adic setting*, J. Number Th., **153** (2015), 63-84.
- [9] R. Barman, H. Rahman and N. Saikia, *Counting points on Dwork hypersurfaces and p -adic hypergeometric functions*, Bull. Aus. Math. Soc., **94** (2016), no. 2, 208-216.
- [10] R. Barman and N. Saikia, *p -adic Gamma function and the trace of Frobenius of elliptic curves*, J. Number Th. **140** (2014), 181-195.
- [11] R. Barman and M. Tripathi, *Certain product formulas and values of Gaussian hypergeometric series*, Res. Number Th. **6** (2020), Art. 26.
- [12] P. Billingsley, *Probability and Measure*, 3rd ed., John Wiley & Sons, Inc. (1995).
- [13] B. J. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc., **43** (1968), 57-60.
- [14] K. Bringmann, A. Folsom, K. Ono, and L. Rolin, *Harmonic Maass forms and mock modular forms: Theory and applications*, Amer. Math. Soc. Colloq. **64**, Amer. Math. Soc., Providence, 2017.
- [15] K. Bringmann, B. Kane, and S. Pujahari, *Distribution of moments of traces of Frobenius in arithmetic progressions and holomorphic projection*, (<https://arxiv.org/pdf/2010.15325.pdf>), preprint.
- [16] L. Clozel, M. Harris, N. Shepherd-Barron, and R. Taylor (2008). *Automorphy for some ℓ -adic lifts of automorphic mod ℓ Galois representations*, Publ. Math. Inst. Hautes Études Sci. **108** (2008), 1-181.
- [17] H. Cohen, *Sums involving the values at negative integers of L -functions of quadratic characters*, Math. Ann., **217** (1975), 271-285.
- [18] H. Cohen and F. Strömberg, *Modular forms: A classical approach*, Graduate Studies in Mathematics, Vol **179**, Amer. Math. Soc., Providence, 2017.
- [19] C. Doran, T. Kelly, A. Salerno, S. Sperber, J. Voight, and U. Whitcher, *Hypergeometric decomposition of symmetric $K3$ quartic pencils*, Res. Math. Sci. **7** (2020), Art. 7.
- [20] M. Eichler, *On the class number of imaginary quadratic fields and the sums of divisors of natural numbers*, J. Indian Math. Soc. **15** (1955), 153-180.
- [21] M. Eichler, *Über die Darstellbarkeit von Modulformen durch Thetareihen*, J. Reine Angew. Math. **195** (1955), 156-171.
- [22] A. El-Guindy, and K. Ono, *Hasse invariants for the Clausen elliptic curves*, Ramanujan J., **31** (1-2) (2013), 3-13.
- [23] F. Fité, K. Kedlaya, and A. V. Sutherland, *Sato-Tate groups of abelian threefolds: a preview of the classification*, Arithmetic Geometry, Cryptography, and Coding Theory, Cont. Math. **770** (2021), Amer. Math. Soc., Providence, 103-129.
- [24] S. Frechette, K. Ono, and M. Papanikolas, *Gaussian hypergeometric functions and traces of Hecke operators*, Int. Math. Res. Not. (**60**) (2004), 3233-3262.
- [25] J. Fuselier, *Hypergeometric functions over \mathbb{F}_p and relations to elliptic curves and modular forms*, Proc. Amer. Math. Soc. **138** (2010), 109-123.
- [26] J. Fuselier, *Traces of Hecke operators in level 1 and Gaussian hypergeometric functions*, Proc. Amer. Math. Soc. **141** (2013), 1871-1881.
- [27] J. Fuselier and D. McCarthy, *Hypergeometric type identities in the p -adic setting and modular forms*, Proc. Amer. Math. Soc. **144** (2016), 1493-1508.
- [28] C. F. Gauss, *Disquisitiones generales circa seriem infinitam $1 + \frac{\alpha\beta}{1\cdot\gamma}x + \frac{\alpha(\alpha+1)\beta(\beta+1)}{1\cdot2\cdot\gamma(\gamma+1)}x^2 + \frac{\alpha(\alpha+1)(\alpha+2)\beta(\beta+1)(\beta+2)}{1\cdot2\cdot3\cdot\gamma(\gamma+1)(\gamma+2)}x^3 + \text{etc.}$* , Cambridge Univ. Press, Cambridge, 2011, 233-279.
- [29] J. Greene, *Character sum analogues for hypergeometric and generalized hypergeometric functions over finite fields*, Thesis (Ph.D.)-University of Minnesota, 1984.
- [30] J. Greene, *Hypergeometric functions over finite fields*, Trans. Amer. Math. Soc. **301** (1) (1987), 77-101.
- [31] J. Greene and D. Stanton, *A character sum evaluation and Gaussian hypergeometric series*, J. Number Theory **23** (1986), 136-148.

- [32] M. Griffin, K. Ono, and W. Tsai *Heights of points on elliptic curves over \mathbb{Q}* , (arXiv:2007.09514v3), Proc. Amer. Math. Soc., accepted for publication.
- [33] D. Husem  ller, *Elliptic curves*, Springer, GTM Vol. 111 (2004).
- [34] K. Ireland and M. Rosen, *A Classical introduction to modern number theory*, 2nd ed, Springer, GTM Vol. 84, New York, (1990).
- [35] M. Ishibashi, H. Sato and K. Shiratani, *On the Hasse invariants of elliptic curves*, Kyushu J. Math., **48** (1994), no. 2, pages 307-321.
- [36] G. Kalita and A. Chetry, *Congruences for generalized Ap  ry numbers and Gaussian hypergeometric series*, Res. Number Th. **3** (2017), Art. 5.
- [37] N. Katz, *Exponential sums and differential equations*, Annals of Math. Studies, Princeton Univ. Press, Princeton, 1990.
- [38] M. Koike, *Orthogonal matrices obtained from hypergeometric series over finite fields and elliptic curves over finite fields*, Hiroshima Math. J. **25** (1995), pages 43-52.
- [39] C. Lennon, *Trace formulas for Hecke operators, Gaussian hypergeometric functions, and the modularity of a threefold*, J. Numb. Th. **131** (2011), 2320-2351.
- [40] C. Lennon, *Gaussian hypergeometric evaluations of traces of Frobenius for elliptic curves*, Proc. Amer. Math. Soc. **139** (2011), 1931-1938.
- [41] W.-C. Li, T. Liu, and L. Long, *Potentially GL_2 -type Galois representations associated to noncongruence modular forms*, Trans. Amer. Math. Soc. **371** (2019), 5341-5377.
- [42] L. Long, R. Ramakrishna, H. Swisher and F.-T. Tu, *Hypergeometric functions over finite fields*, (arXiv:1510.02575v4), preprint (2019).
- [43] D. McCarthy, *${}_3F_2$ hypergeometric series and periods of elliptic curves*, Int. J. of Number Th., **6** (2010), no. 3, pages 461-470.
- [44] D. McCarthy, *On a supercongruence conjecture of Rodriguez-Villegas*, Proc. Amer. Math. Soc. **140** (2012), 2241-2254.
- [45] D. McCarthy, *The trace of Frobenius of elliptic curves and the p -adic Gamma-function*, Pacific J. Math. **261** (2013), 219-236.
- [46] D. McCarthy, *The number of \mathbb{F}_q -points on Dwork hypersurfaces and hypergeometric functions*, Res. in Math. Sci., **4** (2017), no. 4, 1-15.
- [47] D. McCarthy and R. Osburn, *A p -adic analogue of a formula of Ramanujan*, Arch. Math. (Basel) **91** (2008), 492-504.
- [48] D. McCarthy, R. Osburn, and A. Straub, *Sequences, modular forms, and cellular integrals*, Math. Proc. Cambridge Philos. Soc. **168** (2020), 379-404.
- [49] D. McCarthy and M. Papanikolas, *A finite field hypergeometric function associated to eigenvalues of a Siegel eigenform*, Int. J. Number Th. **11** (2015), 2431-2450.
- [50] M. Mertens, *Mock modular forms and class numbers of quadratic forms*, Thesis (Ph.D.)-University of Cologne, 2014, 1-86.
- [51] M. Mertens, *Mock modular forms and class number relations*, Res. Math. Sci. **1** (2014), Art. 6.
- [52] E. Mortenson, *A p -adic supercongruence conjecture of van Hamme*, Proc. Amer. Math. Soc. **136** (2008), 4321-4328.
- [53] K. Ono, *Values of Gaussian hypergeometric series*, Trans. Amer. Math. Soc. **350** (3) (1998), 1205-1223.
- [54] K. Ono, *The web of modularity: Arithmetic of the coefficients of modular forms and q -series*, CBMS, Regional Conference series in Mathematics, 102, Amer. Math. Soc., Providence, 2004.
- [55] R. Osburn and C. Schneider, *Gaussian hypergeometric series and supercongruences*, Math. Comp. **78** (2009), 275-292.
- [56] R. Osburn, B. Sahu, and A. Straub, *Supercongruences for sporadic sequences*, Proc. Edinburgh Math. Soc. **59** (2016), 503-518.
- [57] R. Osburn, A. Straub, and W. Zudilin, *A modular supercongruence for ${}_6F_5$: an Ap  ry-like story*, Ann. Inst. Fourier (Grenoble) **68** (2018), 1987-2004.
- [58] R. Osburn and W. Zudilin, *On the $(K.2)$ supercongruence of Van Hamme*, J. Math. Anal. Appl. **433** (2016), 706-711.
- [59] M. Papanikolas, *A formula and a congruence for Ramanujan's τ -function*, Proc. Amer. Math. Soc. **134** (2006), 333-341.

- [60] L. Pastur and V. Vasilchuk, *On the moments of traces of matrices of classical groups*, Comm. Math. Physics **252** (2004), 149-166.
- [61] S. Pujahari and N. Saikia, *Traces of Hecke operators in level 1 and p -adic hypergeometric functions*, Ramanujan J. **52** (2020), 519-539.
- [62] D. Roberts and F. Rodriguez Villegas, *Hypergeometric motives*, (<https://arxiv.org/abs/2109.00027>), preprint.
- [63] J. Rouse, *Hypergeometric functions and elliptic curves*, Ramanujan J., **12** (2006), no. 2, pages 197-205.
- [64] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Comb. Theory Ser. A **46** (2) (1987), 183-211.
- [65] J. Silverman, *The arithmetic of elliptic curves*, Springer Verlag, New York, 1986.
- [66] F.-T. Tu and Y. Yang, *Evaluation of certain hypergeometric functions over finite fields*, SIGMA **14** (2018), Art. 50.
- [67] D. Zagier, *Nombres de classes et formes modulaires de poids $3/2$* , C. R. Acad. Sci. Paris Sér. A-B **281** (1975), Ai, A883-A886.
- [68] W. Zudilin, *A hypergeometric version of the modularity of rigid Calabi-Yau manifolds*, SIGMA **14** (2018), Art. 86.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF VIRGINIA, CHARLOTTESVILLE, VA 22904

Email address: `ken.ono691@virginia.edu`

Email address: `hs7gy@virginia.edu`

Email address: `nlmsaikia1@gmail.com`