SATO-TATE DISTRIBUTIONS FOR SOME FAMILIES OF HYPERGEOMETRIC VARIETIES

KEN ONO, HASAN SAAD, AND NEELAM SAIKIA

ABSTRACT. At the 2022 RIMS workshop "Algebraic Number Theory and Related Topics," the first author discussed recent work [18, 20] by the authors on Sato-Tate type distributions for two families of elliptic curves and one family of $K3$ surfaces. This is a survey of these results.

1. Introduction and statement of results

In the '80s, Greene [11, 12] developed the foundation of a theory of *hypergeometric functions* over finite fields where these functions possess many properties that are analogous to those of classical hypergeometric functions. Here we study the value distribution of these functions in the context of Sato-Tate distributions for various families of varieties. We first recall Greene's 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 characters of $\mathbb{F}_q^\times$, and where $\binom{A}{B}$ is the normalized Jacobi sum $J(A,B)$, defined by

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

We consider those functions where the characters have order 1 and 2 for $\mathbb{F}_q$ when $q = p^r$ is odd. The simplest example of these functions are the ${}_2F_1$-Gaussian hypergeometric functions

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

where $\phi(\cdot)$ is the quadratic character and ε is the trivial character of $\mathbb{F}_q$.

In [18], the authors computed the moments of these Gaussian hypergeometric functions.

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

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

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

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

The non-zero moments in Theorem 1.1 are Catalan numbers, which also arise [10] as the moments of traces of the Lie group $SU(2)$. In other words, we have

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

where the integral is with respect to the Haar measure on $SU(2)$. Using these moments, we obtain the following limiting distribution.

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

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

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

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

If $\lambda \in \mathbb{F}_q \setminus \{0,1\}$, then (see Theorem 11.10 of [17]) $q \cdot {}_2F_1(\lambda)_q = -\phi(-1) \cdot a_\lambda^{\mathrm{Leg}}(q)$, where

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

Corollary 1.2 refines classical work of Birch [3] which established this distribution for all elliptic curves over finite fields. These distributions coincide with the Sato-Tate distribution that was famously proved by Clozel, Harris, Shepherd-Barron and Taylor in [5]. In their (more difficult) setting, the elliptic curve is fixed and the distribution is taken over all primes p.

We also consider the ${}_3F_2$ Gaussian hypergeometric functions

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

In [18], the authors obtained the following moment asymptotics.

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

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

These are moments [19] of traces of the real orthogonal group $O(3)$ as

$$\int_{O(3)} (\mathrm{Tr} X)^m dX = \sum_{i=0}^m (-1)^i \binom{m}{i} \frac{(2i)!}{i!(i+1)!},$$

where the integral is with respect to the Haar measure on $O(3)$. In analogy with Corollary 1.2, we obtain the limiting distribution.

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

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

where

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

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

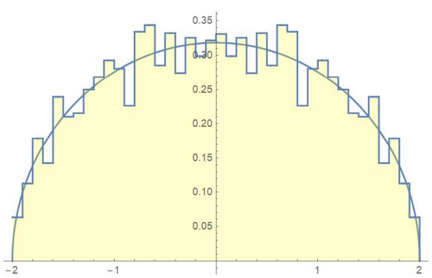
$$X_\lambda : \quad s^2 = xy(x+1)(y+1)(x+\lambda y),$$

where $\lambda \in \mathbb{F}_q \setminus \{0, -1\}$. It is known (see Theorem 11.18 of [17] and Proposition 4.1 of [2]) that

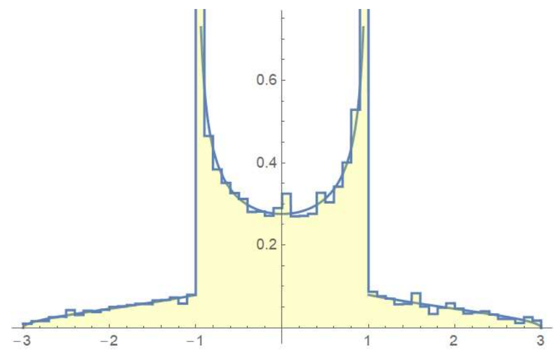
$$|X_\lambda(\mathbb{F}_q)| = 1 + q^2 + 19q + q^2 \cdot {}_3F_2(-\lambda)_q = 1 + q^2 + 19q + q \cdot A_\lambda(p),$$

where $A_\lambda(p) := q \cdot {}_3F_2(-\lambda)_q$. Corollary 1.4 gives the limiting distribution for the $A_\lambda(p)$.

Example. For $p = 93283$, the histograms of the values $\sqrt{p} \cdot {}_2F_1(\lambda)_p$ and $p \cdot {}_3F_2(\lambda)_p$ illustrate Corollary 1.2 and Corollary1.4 (i.e. the near match with the "Batman distribution" $f(t)$).



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



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

In recent work, the second author [20] obtained an explicit version of Theorem 1.3.

Theorem 1.5. *If $-3 \leq a < b \leq 3$ and $p \geq 5$ is a prime, then*

$$\left| \frac{|\{\lambda \in \mathbb{F}_p : A_\lambda(p) \in [a,b]\}|}{p} - \frac{1}{4\pi} \int_a^b f(t)dt \right| \leq \frac{110.84}{p^{1/4}}.$$

This theorem is motivated by the vertical asymptotes at $t = \pm 1$ of the Batman distribution. For example, if $T > 0$, then one can ask how large a prime p must be so that the density of $A_\lambda(p)$ near $t = \pm 1$ is larger than T? As the example above illustrates, $p = 93283$ is not large enough for $T = 1$. More generally, numerical data suggests that the size of such p must grow very rapidly with T. Despite this growth, we have the following explicit bound.

Corollary 1.6. *If $T > \frac{\sqrt{3}}{4\pi}$, $\delta > 0$, and $x(T,\delta) = \frac{4}{1+16\pi^2(T+\delta)^2}$, then the following are true.*

(1) If $p \geq \left(\frac{55.42}{x(T,\delta)\delta}\right)^4$, then

$$\frac{1}{x(T,\delta)} \cdot \frac{|\{\lambda \in \mathbb{F}_p : A_\lambda(p) \in [1 - x(T,\delta), 1]\}|}{p} > T.$$

(2) If $p \geq \left(\frac{55.42}{x(T,\delta)\delta}\right)^4$, *then*

$$\frac{1}{x(T,\delta)} \cdot \frac{|\{\lambda \in \mathbb{F}_p : A_\lambda(p) \in [-1, -1 + x(T,\delta)]\}|}{p} > T.$$

Furthermore, the lower bound on p *is minimal when* $\delta = \frac{\sqrt{16\pi^2 T^2+1}}{4\pi}$.

Example. Suppose that $T = 10$ and $\delta = \frac{\sqrt{1600\pi^2+1}}{4\pi}$. Corollary 1.6 gives that if $p \geq 3.45 \times 10^{14}$ is a prime and $x = 0.00006\ldots$, then we have

$$\frac{1}{x} \cdot \frac{|\{\lambda \in \mathbb{F}_p : A_\lambda(p) \in [1-x, 1]\}|}{p} > 10.$$

As these results are explained in [18] and [20], here we only outline (without proof) the main tools required to obtain Theorems 1.1 and 1.3. The proof of Theorem 1.5 is a significant technical refinement to Theorem 1.3, and we invite the reader to read [20] for the details of its proof.

Acknowledgements

The first author is grateful for the generous hospitality of workshop organizers Tomokazu Kashio and Masataka Chida. He also thanks the Thomas Jefferson Fund and the NSF (DMS-2002265 and DMS-2055118) for their 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. This work was supported by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University.

2. The ${}_2F_1(\lambda)_q$ and the arithmetic of E_λ^{Leg}

2.1. **Facts about Legendre normal forms.**

Here we recall important facts about the ${}_2F_1(\lambda)_q$ values as traces of Frobenius (1.3) of the Legendre normal form elliptic curves E_λ^{Leg}.

Theorem 2.1 (Th. 11.10 of [17])**.** *If* $\lambda \in \mathbb{F}_q \setminus \{0,1\}$ *and* $\mathrm{char}(\mathbb{F}_q) \geq 5$, *then*

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

Remark. Theorem 2.1 is analogous to Gauss' classical hypergeometric formula for the real period $\Omega^{\mathrm{Leg}}(\lambda)$ of E_λ^{Leg} (for example, see Chapter 9 of [13]), where for $0 < \lambda < 1$ we have

$$\pi \cdot {}_2F_1\left(\begin{matrix}\frac{1}{2} & \frac{1}{2} \\ & 1\end{matrix} \mid \lambda\right) = \Omega^{\mathrm{Leg}}(\lambda).$$

By Theorem 2.1, the distribution of the hypergeometric values reduces to a study of family the E_λ^{Leg}. We now recall important facts about these curves.

Proposition 2.2 (Proposition 1.7, Chapter III of [22])**.** *Let* K *be a field with* $\mathrm{char}(K) \neq 2, 3$.
(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*

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

(3) The only λ *for which* $j(E_\lambda^{\mathrm{Leg}}) = 1728$ *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* $K \setminus \{0,1\} \to j(E_\lambda^{\text{Leg}})$ *is six to one. In particular, we have*

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

Since elliptic curves defined over $\mathbb{F}_q$ with the same j-invariant are not necessarily isomorphic over $\mathbb{F}_q$, we must consider their 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

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

then its quadratic twist E_d is given by[1]

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

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

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

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

Proposition 2.3 (Prop. 3.2 of [1])**.** *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, 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

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

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*

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

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* $L(1/2) = \{1/2\}$.

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

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

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

To obtain the power moments of the ${}_2F_1$ hypergeometric functions, we make use of the fact that $\mathbb{Z}2\times\mathbb{Z}2\subseteq E_\lambda^{\mathrm{Leg}}(\mathbb{F}_q)$ and 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 $\mathbb{F}_q$.*

As this 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 $\mathbb{Z}4\times\mathbb{Z}4\subseteq E_\lambda^{\mathrm{Leg}}(\mathbb{F}_q)$ and $E_d\cong E_\lambda^{\mathrm{Leg}}$ 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.

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

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

2.2. **Isomorphism classes of elliptic curves with prescribed subgroups.** We have reformulated the moments as sums over isomorphism classes of elliptic curves for which $\mathbb{Z}2\times\mathbb{Z}2\subseteq E(\mathbb{F}_q)$, and so we seek formulas for the number of such classes. These numbers are known due to work of Schoof [21], and they involve Hurwitz class numbers.

We make this precise. 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 $h(D)=h(\mathcal{O}(-D))$ denote[2] 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

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

where the sum is over all orders $\mathcal{O}'$ between $\mathcal{O}$ and the maximal order $\mathcal{O}_{\max}$. The following theorem of Schoof [21] gives the results we require.

Theorem 2.10 (Section 4 of [21]). *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] We note that $H(D)=H^*(D)=h(D)=0$ whenever $-D$ is neither zero nor a negative discriminant.

(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

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

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 $H\left(\frac{4q-s^2}{n^2}\right)$.

2.3. **Formulas for ${}_2F_1$ moments.** We have the following 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 $q^m \sum_{\lambda \in \mathbb{F}_q} {}_2F_1(\lambda)_q^m = 1$.
(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 $a^{\mathrm{Leg}}(q)_\lambda = \pm 2 \cdot p^{r/2}$. Similarly, $D(q)$ is the average number of such curves in an isomorphism class with $a_\lambda^{\mathrm{Leg}}(q) = 2p^{r/2}$ minus the average number with $a_\lambda^{\mathrm{Leg}}(q) = -2p^{r/2}$.

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} defined by

$$E_\lambda^{\mathrm{Cl}}: \quad y^2 = (x-1)\left(x^2 + \lambda\right). \tag{3.1}$$

Theorem 3.1 (Th. 5 of [16])**.** *If $\lambda \in \mathbb{F}_q \setminus \{0,-1\}$, $\mathrm{char}(\mathbb{F}_q) \geq 5$ and $a_\lambda^{\mathrm{Cl}}(q) := q+1-|E_\lambda^{\mathrm{Cl}}(\mathbb{F}_q)|$, then we have*

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

Remark. Theorem 3.1 has a counterpart in terms of classical hypergeometric functions. For $0 < \lambda < 1$, if $\Omega^{\mathrm{Cl}}(\lambda)$ is the real period of E_λ^{Cl}, then McCarthy [14] proved that

$$ {}_3F_2\left(\begin{matrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ & 1 & 1 \end{matrix} \mid \frac{\lambda}{\lambda+1}\right) = \frac{\sqrt{1+\lambda}}{\pi^2}\cdot \Omega^{\mathrm{Cl}}(\lambda)^2. $$

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

$$ I(s,q) := \{\mathcal{C} \in \mathcal{I}_q \ : \ \forall \ \ E \in \mathcal{C} \text{ we have } |E(\mathbb{F}_q)| = q+1 \pm s\}, \tag{3.2} $$

$$ I_2(s,q) := \{\mathcal{C} \in I(s,q) \ : \ \forall \ E \in \mathcal{C} \text{ we have } E(\mathbb{F}_q)[2] \cong \mathbb{Z}2 \times \mathbb{Z}2\}, \tag{3.3} $$

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

$$ L(s,q) = \left\{\lambda \in \mathbb{F}_q \setminus \{0,-1\} \ : \ a_\lambda^{\mathrm{Cl}}(q) = \pm s\right\}. \tag{3.4} $$

The following proposition gives the moments that will simplify 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

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

(2) If n is a positive integer, then

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

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

The weighted sums of class numbers above arise naturally in the theory of harmonic Maass forms (for background, see [4]). 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 ([23]). *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 on* $\Gamma_0(4)$.

This theorem asserts that the generating function for Hurwitz class numbers [3] is the *holomorphic part* of the harmonic Maass form $\mathcal{H}(\tau)$. More generally (for example, see Lemma 4.3 of [4]), every weight $k \neq 1$ harmonic weak Maass form $f(\tau)$ has a Fourier expansion of the form

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

where

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

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.

Our weighted sums of class numbers appear in the coefficients of certain families of nonholomorphic modular forms. These forms are constructed from Zagier's $\mathcal{H}(\tau)$ via the Rankin-Cohen bracket operators, which are combinatorial expressions in derivatives of pairs of modular forms.

4.1. Families of modular forms obtained from Rankin-Cohen brackets.

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 νth *Rankin-Cohen bracket* of f and g is

$$[f, g]_\nu := \frac{1}{(2\pi i)^\nu} \sum_{r+s=\nu} (-1)^r \binom{k+\nu-1}{s} \binom{l+\nu-1}{r} \frac{d^r}{d\tau^r} f \cdot \frac{d^s}{d\tau^s} g. \tag{4.3}$$

These operators preserve modularity.

Proposition 4.2 (Th. 7.1 of [6]). *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 4.2 (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 $\nu > 0$.

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

Proposition 4.2 is a procedure for producing many nonholomorphic modular forms from derivatives of a pair of seed forms f and g. We study forms that arise in this way from $f(\tau) := \mathcal{H}(\tau)$ and certain univariate theta functions for $g(\tau)$. To prove Theorem 1.1 and 1.3, 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 $f : \mathbb{H} \to \mathbb{C}$ 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 $\{\kappa_1, \ldots, \kappa_M\}$ be the cusps of Γ, where $\kappa_1 := i\infty$. Moreover, for each j let $\gamma_j \in \mathrm{SL}_2(\mathbb{Z})$ 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

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

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

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

$$(\pi_{\mathrm{hol}} f)(\tau) := c_0 + \sum_{n=1}^{\infty} c(n) q_\tau^n, \tag{4.4}$$

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 4.3 (Prop. 10.2 of [4]). *Assuming the hypotheses above, if $k > 2$ (resp. $k = 2$), then $\pi_{hol}(f)$ 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 4.3 has the following convenient decomposition

$$\pi_{\mathrm{hol}}([f, g]_\nu) = [f^+, g]_\nu + \frac{(4\pi)^{1-k}}{k-1} \overline{c_f^-(0)} \pi_{\mathrm{hol}}([y^{1-k}, g]_\nu) + \pi_{\mathrm{hol}}([f^-, g]_\nu). \tag{4.5}$$

For our applications, the weighted class number sums will arise from the first summand $[f^+, g]_\nu$ of (4.5), 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 (4.5) must be bounded for our applications.

5. Bounds for weighted sums of class numbers

Here we state 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.

5.1. **Some Standard Bounds.** Here we recall 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 $p \to +\infty$, 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 $\Omega_{p^r} := \{s \in [-2\sqrt{p^r}, 2\sqrt{p^r}] \ : \ p \mid s \text{ and } s \equiv p^r + 1 \pmod 4\}$.

Theorem 5.2 (Remark 9.3.15 of [7])**.** *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. **Asymptotics for weighted sums of class numbers.** Using the results from the previous two sections (i.e. Rankin-Cohen brackets, combinatorial identities, class number bounds, Deligne's Theorem, and holomorphic projection), one can derive the asymptotic formulas which are crucial for the proof of Theorem 1.1. A large portion of [18] is devoted to the proof of the following three lemmas along these lines.

Lemma 5.3. *If n is a nonnegative integer, then*

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

Lemma 5.4. *If m is a positive odd integer, then the following are true.*
(1) As $q \to \infty$ 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 $q \to \infty$ with $q \equiv 1 \pmod 4$, we have

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

Lemma 5.5. *If n is a nonnegative integer, then as $q \to +\infty$ we have*

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

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

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

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

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

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

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

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

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

where

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

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 5.3 and 5.4, thereby concluding the proof. □

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

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

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

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 [12]), Theorem 3.1 gives us that

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

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

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

References

[1] S. Ahlgren and K. Ono, *Modularity of a certain Calabi-Yau threefold*, Montash. Math. **129** (3) (2000), 177–190.

[2] S. Ahlgren, K. Ono, and D. Penniston, *Zeta functions of an infinite family of $K3$ surfaces*, Amer. J. Math., **124** (2) (2002), 353–368.

[3] 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.

[4] K. Bringmann, A. Folsom, K. Ono, and L. Rolen, *Harmonic Maass forms and mock modular forms: Theory and applications*, Amer. Math. Soc. Colloq. **64**, Amer. Math. Soc., Providence, 2017.

[5] 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.

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

[7] H. Cohen and F. Strömberg, *Modular forms: A classical approach*, Graduate Studies in Mathematics, Vol **179**, Amer. Math. Soc., Providence, 2017.

[8] 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.

[9] M. Eichler, *Über die Darstellbarkeit von Modulformen durch Thetareihen*, J. Reine Angew. Math. **195** (1955), 156-171.

[10] 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.

[11] J. Greene, *Character sum analogues for hypergeometric and generalized hypergeometric functions over finite fields*, Thesis (Ph.D.)-University of Minnesota, 1984.

[12] J. Greene, *Hypergeometric functions over finite fields*, Trans. Amer. Math. Soc. **301** (1) (1987), 77–101.

[13] D. Husemöller, *Elliptic curves*, Springer, GTM Vol. 111 (2004).

[14] D. McCarthy, *${}_3F_2$ hypergeometric series and periods of elliptic curves*, Int. J. of Number Th., **6** (2010), no. 3, pages 461-470.

[15] M. Mertens, *Mock modular forms and class numbers of quadratic forms*, Thesis (Ph.D.)-University of Cologne, 2014, 1–86.

[16] K. Ono, *Values of Gaussian hypergeometric series*, Trans. Amer. Math. Soc. **350** (3) (1998), 1205–1223.

[17] 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.

[18] K. Ono, H. Saad, and N. Saikia, *Distribution of values of Gaussian hypergeometric functions*, Pure and Applied Mathematics Quarterly, accepted for publication.

[19] L. Pastur and V. Vasilchuk, *On the moments of traces of matrices of classical groups*, Comm. Math. Physics **252** (2004), 149-166.

[20] H. Saad, *Explicit Sato-Tate type distributions for a family of $K3$ surfaces*, submitted for publication.

[21] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Comb. Theory Ser. A **46** (2) (1987), 183–211.

[22] J. Silverman, *The arithmetic of elliptic curves*, Springer Verlag, New York, 1986.

[23] 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.

Department of Mathematics, University of Virginia, Charlottesville, VA 22904
Email address: `ken.ono691@virginia.edu`
Email address: `hs7gy@virginia.edu`

School of Basic Sciences, Indian Institute of Techonology Bhubaneswar, Argul, Khorda 752050, Odisha, India
Email address: `nlmsaikia1@gmail.com`