ODD MOMENTS FOR THE TRACE OF FROBENIUS AND THE SATO–TATE CONJECTURE IN ARITHMETIC PROGRESSIONS

KATHRIN BRINGMANN, BEN KANE, AND SUDHIR PUJAHARI

ABSTRACT. In this paper, we consider the moments of the trace of Frobenius of elliptic curves if the trace is restricted to a fixed arithmetic progression. We determine the asymptotic behavior for the ratio of the $(2k + 1)$-th moment to the zeroeth moment as the size of the finite field $\mathbb{F}_{p^r}$ goes to infinity. These results follow from similar asymptotic formulas relating sums and moments of Hurwitz class numbers where the sums are restricted to certain arithmetic progressions. As an application, we prove that the distribution of the trace of Frobenius in arithmetic progressions is equidistributed with respect to the Sato–Tate measure.

1. INTRODUCTION AND STATEMENT OF THE RESULTS

For an elliptic curve E over the finite field $\mathbb{F}_{p^r}$ with p^r elements, there is a natural endomorphism called the Frobenius map. Letting $\mathrm{tr}(E) := p^r + 1 - \#E(\mathbb{F}_{p^r})$ be the *trace of Frobenius*, Hasse [10] proved that $|\mathrm{tr}(E)| \leq 2p^{\frac{r}{2}}$. The normalized trace of Frobenius

$$x_E := \frac{\mathrm{tr}(E)}{2p^{\frac{r}{2}}}$$

is hence an element of $[-1, 1]$. It is then natural to investigate the distribution of $x_E \in [-1, 1]$ as $p^r \to \infty$. Birch [2] related this distribution to the *Sato–Tate measure* $\mu_{\mathrm{ST}}(X) := \int_X f_{\mathrm{ST}}(x)dx$, where $X \subseteq \mathbb{R}$ is a Lebesgue integrable set and

$$f_{\mathrm{ST}}(x) := \begin{cases} \frac{2}{\pi}\sqrt{1 - x^2} & \text{if } x \in [-1, 1], \\ 0 & \text{otherwise.} \end{cases}$$

Specifically, letting $E_{\alpha,\beta}$ denote the elliptic curve in Weierstrass form $y^2 = x^3 - \alpha x - \beta$ for $\alpha, \beta \in \mathbb{F}_p$, Birch [2] proved that for $-1 \leq a \leq b \leq 1$ we have

$$\lim_{p\to\infty} \Pr\left(a \leq x_{E_{\alpha,\beta}} \leq b : \alpha, \beta \in \mathbb{F}_p\right) = \mu_{\mathrm{ST}}([a, b]).$$

Here, as usual, for a finite set $\mathcal{E}$ and a statement $\mathcal{S}(x)$ (which is true or false for each $x \in \mathcal{E}$), we define the probability of the event $\mathcal{S}$ in the sample space $\mathcal{E}$ to be

$$\Pr\left(\mathcal{S}(x) : x \in \mathcal{E}\right) := \frac{\#\left\{x \in \mathcal{E} : \mathcal{S}(x) \text{ holds}\right\}}{\#\mathcal{E}}.$$

We say that the set of x_E for $E \in \{E_{\alpha,\beta} : \alpha, \beta \in \mathbb{F}_p\}$ become *equidistributed* with respect to the Sato–Tate measure as $p \to \infty$. Birch's result has been extended to the case where $\mathbb{F}_p$ is replaced with an arbitrary finite field $\mathbb{F}_{p^r}$ (see the work of Brock and Granville [4] as well as [15]). Instead of considering the sample space defined by the coefficients of the cubic polynomial, we investigate subsets of the set $\mathcal{E}(p^r)$ of equivalence classes of elliptic curves over $\mathbb{F}_{p^r}$. Specifically, for $m \in \mathbb{Z}$ and $M \in \mathbb{N}$, we generalize Birch's result by considering the sample space

$$\mathcal{E}_{m,M}(p^r) := \{E \in \mathcal{E}(p^r) : \operatorname{tr}(E) \equiv m \pmod{M}\}.$$

Theorem 1.1. *Let $m \in \mathbb{Z}$ and $M, r \in \mathbb{N}$. Restricting to $E \in \mathcal{E}_{m,M}$ over $\mathbb{F}_{p^r}$, the normalized traces of Frobenius x_E are equidistributed with respect to the Sato–Tate measure in the interval $[-1, 1]$ as $p \to \infty$. Specifically, we have*

$$\lim_{p \to \infty} \Pr\left(a \le x_E \le b : E \in \mathcal{E}_{m,M}(p^r)\right) = \mu_{\mathrm{ST}}([a, b]).$$

It is also natural to consider the analogous question for the probabilities

$$\Pr\left(a \le x_E \le b \text{ and } E \in \mathcal{E}_{m,M}(p^r) : E \in \mathcal{E}(p^r)\right) \tag{1.1}$$

on the larger sample space $\mathcal{E}(p^r)$. Since the distribution of x_E in $[-1, 1]$ is the same on the sample spaces $\mathcal{E}(p^r)$ and $\mathcal{E}_{m,M}(p^r)$ as $p \to \infty$, Theorem 1.1 shows that as $p \to \infty$ the set of x_E becomes equidistributed independent of the distribution of $\operatorname{tr}(E)$ modulo M. The distribution of $\operatorname{tr}(E)$ modulo M was studied by Castryck and Hubrechts [5]. In particular, for fixed m and M, they determined [5, Theorem 1] the asymptotic behavior of

$$\Pr\left(E \in \mathcal{E}_{m,M}(p^r) : E \in \mathcal{E}(p^r)\right), \tag{1.2}$$

up to an error of size $O_M(p^{-\frac{r}{2}})$. Given the independence of the distribution of x_E and the distribution of $\operatorname{tr}(E)$ modulo M as $p \to \infty$, (1.1) converges to (1.2) times the Sato–Tate distribution. While the limit as $p \to \infty$ of (1.2) (and hence (1.1)) does not exist in general, the limit exists under certain restrictions. We list one such case in the following theorem.

Theorem 1.2. *Let $m \in \mathbb{Z}$ and $M, r \in \mathbb{N}$. Then for each $j \in \mathbb{Z}$ with $\gcd(j, 2M) = 1$ there exists a constant $c_{j,m,M}$ such that the normalized traces x_E ($E \in \mathcal{E}_{m,M}$) are each equidistributed in $[-1, 1]$ within the larger space with respect to the measure $c_{j,m,M}\mu_{\mathrm{ST}}$ as $p \to \infty$ with $p \equiv j \pmod{4M^2}$. Specifically, for $-1 \le a \le b \le 1$ we have*

$$\lim_{\substack{p \to \infty \\ p \equiv j \pmod{4M^2}}} \Pr\left(a \le x_E \le b \text{ and } E \in \mathcal{E}_{m,M}(p) : E \in \mathcal{E}(p)\right) = c_{j,m,M}\mu_{\mathrm{ST}}([a, b]).$$

Remark. With a little more work, one should be able to determine the limiting distribution coming from taking $p \to \infty$ in (1.1) by using the evaluation of (1.2) in [5, Theorem 1].

In order to investigate the distributions in Thorems 1.1 and 1.2 , we use the method of moments (see Section 2.5), which relies on the fact that a reasonable probability measure is determined by its nonnegative integer moments. We investigate closely-related weighted moments that converges to the unweighted moments as $p \to \infty$ (see Section 2.6). To describe the weighting, denote by $\operatorname{Aut}_{\mathbb{F}_{p^r}}(E)$ the automorphism group of $E/\mathbb{F}_{p^r}$ and set $\omega_E := \#\operatorname{Aut}_{\mathbb{F}_{p^r}}(E)$. In particular, we show that for $\nu \in \mathbb{N}_0$ the weighted moments of x_E

$$\sum_{\substack{E/\mathbb{F}_{p^r} \\ \operatorname{tr}(E) \equiv m \pmod{M}}} \frac{x_E^\nu}{\omega_E} = \frac{1}{2^\nu p^{\frac{r\nu}{2}}} S_{\nu,m,M}(p^r) \tag{1.3}$$

converge to the moments of μ_{ST}, where

$$S_{\nu,m,M}(p^r) := \sum_{\substack{E/\mathbb{F}_{p^r} \\ \mathrm{tr}(E) \equiv m \ (\mathrm{mod}\ M)}} \frac{\mathrm{tr}(E)^\nu}{\omega_E}. \tag{1.4}$$

The weighted even moments $\nu \in 2\mathbb{N}_0$ have been studied by a number of authors such as [2, 3, 12, 13, 14, 17, 20]. For example, in [3, Theorem 1.1] it was shown that as $p \to \infty$ (if $\nu = 0$, we omit the subscript throughout)

$$\frac{S_{2k,m,M}(p)}{2^{2k} p^k S_{m,M}(p)} = \frac{C_k}{2^{2k}} + O\left(p^{-\frac{1}{2}+\varepsilon}\right), \quad \frac{S_{2k,m,M}(p^r)}{2^{2k} p^{rk} S_{m,M}(p^r)} = \frac{C_k}{2^{2k}} + O\left(p^{-1+\varepsilon}\right) \ (r \geq 2), \tag{1.5}$$

where $C_k := \frac{(2k)!}{k!(k+1)!}$ is the k-th *Catalan number*. Since the main term in (1.5) matches the $2k$-th moment of μ_{ST} (see Lemma 2.4), it remains to study the odd moments. In the case $M = 1$, all of the odd moments vanish due to a symmetry which implies that (see [14, Theorem 3])

$$\sum_{\substack{E/\mathbb{F}_{p^r} \\ \mathrm{tr}(E)=-t}} \omega_E^{-1} = \sum_{\substack{E/\mathbb{F}_{p^r} \\ \mathrm{tr}(E)=t}} \omega_E^{-1}.$$

For $M > 1$, this symmetry is broken, but we prove in this paper that there is still a large amount of cancellation. We both vary the prime p and the power r, getting equivalent cancellation in both cases.

Theorem 1.3. *Let $k \in \mathbb{N}$, $m \in \mathbb{Z}$, and $M \in \mathbb{N}$ be given.*
(1) *For a fixed prime $p > 3$, as $r \to \infty$ we have*

$$S_{2k+1,m,M}(p^r) = O_{k,M,\varepsilon}\left(p^{(k+1+\varepsilon)r}\right).$$

(2) *For $r \in \mathbb{N}$ fixed, as $p \to \infty$ we have*

$$S_{2k+1,m,M}(p^r) = O_{k,M,\varepsilon}\left(p^{(k+1+\varepsilon)r}\right).$$

Remarks.
(1) Using (1.3), Theorem 1.3 implies that

$$\frac{1}{S_{m,M}(p^r)} \sum_{\substack{E/\mathbb{F}_{p^r} \\ \mathrm{tr}(E) \equiv m \ (\mathrm{mod}\ M)}} \frac{x_E^{2k+1}}{\omega_E} = O_{k,M,\varepsilon}\left(p^{(-\frac{1}{2}+\varepsilon)r}\right). \tag{1.6}$$

Here we use the fact that

$$S_{m,M}(p^r) \gg_{M,\varepsilon} p^{(1-\varepsilon)r}, \tag{1.7}$$

which follows by plugging [3, Lemma 3.7] and [3, Lemma 4.2] into [3, Lemma 2.2].
(2) By Birch's result [2] and its generalizations [4, 15], for any constant $0 < c < 2$ the set

$$\#\left\{E/\mathbb{F}_{p^r} : |\mathrm{tr}(E)| > cp^{\frac{r}{2}}\right\}$$

has positive density in $E/\mathbb{F}_{p^r}$ as $p^r \to \infty$. Hence if one takes the moments in (1.4) with $\mathrm{tr}(E)$ replaced with $|\mathrm{tr}(E)|$, then

$$\sum_{\substack{E/\mathbb{F}_{p^r} \\ \mathrm{tr}(E) \equiv m \ (\mathrm{mod}\ M)}} \frac{|\mathrm{tr}(E)|^\nu}{\omega_E} \geq \sum_{\substack{E/\mathbb{F}_{p^r} \\ \mathrm{tr}(E) \equiv m \ (\mathrm{mod}\ M) \\ \mathrm{tr}(E) > cp^{\frac{r}{2}}}} \frac{\mathrm{tr}(E)^\nu}{\omega_E} \gg_{c,\nu} p^{\frac{r\nu}{2}} S_{m,M}(p^r) \gg_{M,\varepsilon} p^{(\frac{\nu}{2}+1-\varepsilon)r}.$$

3

In the last inequality, we use the bound (1.7) again. Taking $\nu = 2k + 1$, we conclude that if no cancellation would occur in $S_{2k+1,m,M}(p^r)$, then we would have

$$S_{2k+1,m,M}(p^r) \gg p^{r(k+\frac{3}{2}-\varepsilon)}.$$

We hence see that the cancellation yields a power savings of (at least) $p^{(\frac{1}{2}-\varepsilon)r}$.

Our investigation of the moments related to the trace of Frobenius goes through moments associated to class numbers of imaginary quadratic fields, or, equivalently, the *Hurwitz class numbers* $H(n)$ for classes of binary quadratic forms, which we next define. For $n \in \mathbb{N}$, we let $H(n)$ denote the number of $\mathrm{SL}_2(\mathbb{Z})$-inequivalent classes of integral binary quadratic forms $[a, b, c]$ of discriminant $-n$, counted with multiplicity $\frac{1}{2}$ if $[a, b, c]$ is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to $[a, 0, a]$ and multiplicity $\frac{1}{3}$ if $[a, b, c]$ is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to $[a, a, a]$. We furthermore set $H(0) := -\frac{1}{12}$ and $H(n) := 0$ for $n < 0$. For $\nu \in \mathbb{N}_0$, $M \in \mathbb{N}$, $m \in \mathbb{Z}$, and $n \in \mathbb{N}_0$, we define

$$H_{\nu,m,M}(n) := \sum_{t \equiv m \pmod{M}} H\left(4n - t^2\right) t^\nu. \tag{1.8}$$

Analogously to the remark after Theorem 1.3, if one replaces t with $|t|$ in (1.8), then the main contribution is expected to come from t of size roughly $|t| \approx \sqrt{n}$. Hence it is natural to divide (1.8) by the expected average absolute value (abbreviating $H_{m,M}(n) := H_{0,m,M}(n)$)

$$n^{\frac{\nu}{2}} \sum_{t \equiv m \pmod{M}} H\left(4n - t^2\right) = n^{\frac{\nu}{2}} H_{m,M}(n).$$

Indeed, in [3, Theorem 1.3], it was shown that for $k \in \mathbb{N}_0$

$$\frac{H_{2k,m,M}(n)}{n^k H_{m,M}(n)} = C_k + O_{k,M,\varepsilon}\left(n^{-\frac{1}{2}+\varepsilon}\right).$$

Combining this with [3, Lemma 3.7], one also obtains

$$H_{2k,m,M}(n) = C_k n^k H_{m,M}(n) + O_{k,M,\varepsilon}\left(n^{k+\frac{1}{2}+\varepsilon}\right). \tag{1.9}$$

Since t^ν alternates in sign for odd ν, one again expects cancellation. We show that this happens in the following theorem.

Theorem 1.4. *Let $k \in \mathbb{N}_0$ be given. Then*

$$\frac{H_{2k+1,m,M}(n)}{n^{k+\frac{1}{2}} H_{m,M}(n)} = O_{k,M,\varepsilon}\left(n^{-\frac{1}{2}+\varepsilon}\right), \quad H_{2k+1,m,M}(n) = O_{k,M,\varepsilon}\left(n^{k+1+\varepsilon}\right).$$

Remark. Combining Theorem 1.4 with (1.9), for $\nu \in \mathbb{N}_0$ we have

$$H_{\nu,m,M}(n) = \delta_{2|\nu} C_{\frac{\nu}{2}} n^{\frac{\nu}{2}} H_{m,M}(n) + O_{\nu,M,\varepsilon}\left(n^{\frac{\nu+1}{2}+\varepsilon}\right),$$

where $\delta_S := 1$ if a statement S holds and $\delta_S := 0$ otherwise.

The paper is organized as follows. In Section 2, we give background information. In Section 3, we evaluate the coefficients of the Rankin–Cohen brackets between the Hurwitz class number generating function and a weight $\frac{3}{2}$ unary theta function. The Rankin–Cohen brackets are then related to the odd moments in Section 4, where Theorem 1.4 is proven. We show Theorem 1.3 in Section 5. Finally, we consider the applications to distributions of the trace of Frobenius in Section 6, proving Theorem 1.1 and Theorem 1.2.

2. Preliminaries

2.1. Holomorphic and non-holomorphic modular forms.
We give a brief overview of the theory of modular forms here; for details, see e.g. [16, 21]. We assume throughout that $\Gamma \subseteq \Gamma_0(4)$ is a congruence subgroup containing $T := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\kappa \in \frac{1}{2}\mathbb{Z}$. For d odd, we set

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

and we denote the extended Legendre symbol by $\left(\frac{\cdot}{\cdot}\right)$. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ we define the weight κ *slash operator* by

$$F\big|_\kappa \gamma(\tau) := \left(\frac{c}{d}\right)^{2\kappa} \varepsilon_d^{2\kappa}(c\tau + d)^{-\kappa} F(\gamma\tau).$$

A function $F : \mathbb{H} \to \mathbb{C}$ satisfies *modularity of weight κ on Γ with character χ* if for every $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ we have

$$F|_\kappa \gamma = \chi(d)F.$$

We call F a *(holomorphic) modular form* if F is holomorphic on $\mathbb{H}$ and $F(\tau)$ grows at most polynomially in v as $\tau = u + iv \to \mathbb{Q} \cup \{i\infty\}$. We say that $F : \mathbb{H} \to \mathbb{C}$ is an *almost holomorphic modular form* if F satisfies weight κ modularity on Γ and there exist holomorphic functions F_j ($0 \le j \le \ell$) such that $F(\tau) = \sum_{j=0}^\ell F_j(\tau)v^{-j}$. We call F_0 a *quasimodular form*.

2.2. Rankin–Cohen brackets.
For F_1, F_2 transforming like modular forms of weight $\kappa_1, \kappa_2 \in \frac{1}{2}\mathbb{Z}$, respectively, define for $k \in \mathbb{N}_0$ the k-th *Rankin-Cohen bracket*

$$[F_1, F_2]_k := \frac{1}{(2\pi i)^k} \sum_{j=0}^k (-1)^j \binom{\kappa_1 + k - 1}{k - j} \binom{\kappa_2 + k - 1}{j} F_1^{(j)} F_2^{(k-j)}$$

with $\binom{\alpha}{j} := \frac{\Gamma(\alpha+1)}{j!\Gamma(\alpha-j+1)}$. Here the *gamma function* is defined by $\Gamma(s) := \int_0^\infty t^{s-1}e^{-t}dt$ for $\mathrm{Re}(s) > 0$ (and via meromorphic continuation for $s \in \mathbb{C}$). Cohen showed in [6, Theorem 7.1 (a)] that $[F_1, F_2]_k$ transforms like a modular form of weight $\kappa_1 + \kappa_2 + 2k$.

2.3. Holomorphic projection.
Suppose that we have a (not necessarily holomorphic) translation-invariant function $F(\tau) = \sum_{n \in \mathbb{Z}} c_{F,v}(n)q^n$. In [25], Sturm observed that if F satisfies modularity of weight $\kappa \ge 2$ on some congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ and $\langle F, g \rangle$ exists for every cusp form g of weight κ on Γ, then there exists a unique cusp form f (in the same space) such that $\langle F, g \rangle = \langle f, g \rangle$ for every g. Sturm called this cusp form f the *holomorphic projection* of F and evaluated its Fourier coefficients as a certain integral. Gross and Zagier (see [9, Proposition 5.1, p. 288]) instead used Sturm's evaluation via an integral as the definition of the holomorphic projection operator, which extends to a more general setting. Following the construction of [9], we now relax the condition on F, dropping the assumption that it is modular and only assuming that it is translation-invariant. If $c_{F,v}(n) \ll_{F,n} v^{2-\kappa}$ as $v \to 0^+$ for all $n \in \mathbb{N}$, then for $n \in \mathbb{N}$ we define

$$c_F(n) := \frac{(4\pi n)^{\kappa-1}}{\Gamma(\kappa-1)} \int_0^\infty c_{F,v}(n)v^{\kappa-2}e^{-4\pi nv}dv.$$

If there exists a constant $c_F(0) \in \mathbb{C}$ for which $F(\tau) - c_F(0)$ decays as $\tau \to i\infty$, and if a similar condition holds as $\tau \to \mathbb{Q}$, we define (see [19] for the statement written in this generality) the *holomorphic projection* of F as

$$\pi_{\mathrm{hol}}(F)(\tau) := c_F(\kappa, 0) + \sum_{n=1}^\infty c_F(n)q^n.$$

Although we may apply holomorphic projection with any κ satisfying the growth conditions, one usually applies the holomorphic projection operator to a function F satisfying modularity of weight κ, but then writes $F = \sum_{j=1}^{\ell} F_j$, so the weight κ is clear from the context. Using this more general definition above to apply the operator to the individual summands F_j even though they may not be modular.

Mertens [18] studied the holomorphic projection of the Rankin–Cohen brackets between holomorphic modular forms and non-holomorphic modular forms with Fourier expansions of the type

$$F(\tau) = F^+(\tau) + F^-(\tau) \tag{2.1}$$

with (for $q := e^{2\pi i \tau}$)

$$F^+(\tau) = \sum_{n \gg -\infty} c_F^+(n) q^n, \qquad F^-(\tau) = c_F^-(0) v^{1-\kappa} + \sum_{n \leq -1} c_F^-(n) \Gamma\left(1 - \kappa, 4\pi |n| v\right) q^n.$$

Here for $x > 0$ and $\alpha \in \mathbb{C}$, denote by $\Gamma(\alpha, x) =: \int_x^\infty t^{\alpha-1} e^{-t} dt$ the *incomplete gamma function*. We set

$$F_0^-(\tau) := F^-(\tau) - c_F^-(0) v^{1-\kappa}.$$

We require the contribution to this holomorphic projection coming from the non-holomorphic part, which was given in [18, Lemma 4.4 and Theorem 4.6]. To state it, for $a \in \mathbb{N}$ and $b \in \mathbb{R}$ we define the two-variable polynomials

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

Moreover, for $\kappa_1, \kappa_2 \in \mathbb{R} \setminus \mathbb{Z}$ and $k \in \mathbb{N}_0$ with $2k - 2 \geq \kappa_1 + \kappa_2 \in \mathbb{Z}$, we define

$$\alpha_{\kappa_1, \kappa_2, k} := \frac{1}{(\kappa_1 + \kappa_2 + 2k - 2)!(\kappa_1 - 1)} \sum_{\mu=0}^{k} \frac{\Gamma(2 - \kappa_1)\Gamma(\kappa_2 + 2k - \mu)}{\Gamma(2 - \kappa_1 - \mu)} \binom{\kappa_1 + k - 1}{k - \mu} \binom{\kappa_2 + k - 1}{\mu}.$$

Lemma 2.1. *Let* $\kappa_1, \kappa_2 \in \mathbb{Z} + \frac{1}{2}$ *and* $k \in \mathbb{N}_0$ *with* $2k - 2 \geq \kappa_1 + \kappa_2 \in \mathbb{Z}$ *be given. Suppose that* F *satisfies modularity of weight* κ_1 *and has a Fourier expansion of the type* (2.1) *that grows at most polynomially towards the cusps and* g *is a holomorphic modular form of weight* κ_2. *Applying holomorphic projection in weight* $\kappa_1 + \kappa_2 + 2k$ *to* $[F, g]_k$ *and splitting* F *as in* (2.1), *we have the following.*

(1) *We have*

$$\frac{(4\pi)^{1-\kappa_1}}{\kappa_1 - 1} \pi_{\text{hol}}\left(\left[v^{1-\kappa_1}, g\right]_k\right) = \alpha_{\kappa_1, \kappa_2, k} \sum_{n=0}^{\infty} n^{\kappa_1 + k - 1} c_g(n) q^n.$$

(2) *We have*

$$\pi_{\text{hol}}\left(\left[F_0^-, g\right]_k\right)(\tau) = \sum_{n=1}^{\infty} b(n) q^n,$$

where

$$b(n) = -\Gamma(1 - \kappa_1) \sum_{\substack{j, \ell \in \mathbb{N} \\ j - \ell = n}} \sum_{\mu=0}^{k} \binom{k_1 + k - 1}{k - \mu} \binom{k_2 + k - 1}{\mu} j^{k-\mu} c_g(j) \frac{c_F^-(-\ell)}{\ell^{\kappa_1 - 1}}$$

$$\times \left(j^{\mu - 2k - \kappa_2 + 1} P_{\kappa_1 + \kappa_2 + 2k, 2 - \kappa_1 - \mu}(n, \ell) - \ell^{\kappa_1 + \mu - 1}\right).$$

6

2.4. **Examples of modular objects.** We require a few specific modular objects. We first define

$$\theta_{\nu,m,M}(\tau) := \sum_{n \equiv m \pmod M} n^\nu q^{n^2},$$

Setting $\Gamma_{N,M} := \Gamma_0(N) \cap \Gamma_1(M)$ for $M \mid N$, this is a quasimodular form of weight $\nu + \frac{1}{2}$ on $\Gamma_{4M^2,M}$ (see [23, Proposition 2.1]). It is moreover a holomorphic modular form for $\nu = 0$ and a cusp form for $\nu = 1$. Let

$$\mathcal{H}(\tau) := \sum_{n \in \mathbb{Z}} H(n) q^n$$

be the generating function for the Hurwitz class numbers. Its modular properties follow by [11, Theorem 2].

Theorem 2.2. *The function*

$$\widehat{\mathcal{H}}(\tau) := \mathcal{H}(\tau) + \frac{1}{8\pi\sqrt{v}} + \frac{1}{4\sqrt{\pi}} \sum_{n=1}^{\infty} n\Gamma\left(-\frac{1}{2}, 4\pi n^2 v\right) q^{-n^2}$$

is a non-holomorphic modular form of weight $\frac{3}{2}$ on $\Gamma_0(4)$ which grows at most polynomially towards all cusps and has an expansion of the type (2.1).

2.5. **Equidistribution and the method of moments.**

Definition 2.3. Let f be a real-valued continuous function with compact support. We define a measure μ_f on integrable sets X by

$$\mu_f(X) := \int_X f(x)dx.$$

In the special case $f = f_{\mathrm{ST}}$, we write $\mu_{\mathrm{ST}} = \mu_{f_{\mathrm{ST}}}$ for ease of notation. We say that a sequence of subsets $S_j \subseteq \mathbb{R}$ is *equidistributed with respect to μ_f* if for every $a \le b$ we have

$$\lim_{j \to \infty} \mathrm{Pr}\left(a \le x \le b : x \in S_j\right) = \int_a^b f(x)dx = \mu_f([a,b]).$$

We investigate μ_f through the *ν-th moment of f at* 0, which is defined by

$$\mu_{f,\nu} := \int_{-\infty}^{\infty} x^\nu f(x)dx.$$

In the special case $f = f_{\mathrm{ST}}$, we write $\mu_{\mathrm{ST},\nu}$. Suppose now that f is a probability density function and let X be a random variable corresponding to f; i.e., X randomly assigns a value in $\mathbb{R}$ such that for $a < b$

$$\mathrm{Pr}\left(a \le X \le b\right) = \int_a^b f(x)dx.$$

Recall that for a function $g : \mathbb{R} \to \mathbb{R}$, the *expected value of $g(X)$* is

$$E[g(X)] := \int_{-\infty}^{\infty} g(x)f(x)dx.$$

In this case, we see that the ν-th moment is

$$E[X^\nu] = \mu_{f,\nu}.$$

Under certain mild conditions, the moments of a distribution uniquely determine the distribution (see [1, Theorem 30.1 and Theorem 30.2]). In order to prove Theorem 1.1, we require the moments of the Sato–Tate measure, which are well-known (for example, see the introduction of [2]).

Lemma 2.4. *For $k \in \mathbb{N}_0$, the $2k$-th moment of the Sato–Tate distribution is*

$$\mu_{\mathrm{ST},2k} = \frac{C_k}{2^{2k}},$$

while $\mu_{\mathrm{ST},2k+1} = 0$.

2.6. **Weighted distributions and equidistribution.** By determining when two of the elliptic curves $E_{\alpha,\beta}$ are equivalent (see [2, discussion after (1)]), Birch's result and its generalizations may be naturally described using a weighted probability on $\mathcal{E}(p^r)$. For a statement $\mathcal{S}(E)$ which is true or false for each E in a subset $\mathcal{E}$ of elliptic curves over $\mathbb{F}_{p^r}$, we set $\mathcal{E}_{\mathcal{S}} := \{E \in \mathcal{E} : \mathcal{S}(E) \text{ holds}\}$ and set

$$\mathrm{Pr}_{\mathrm{Aut}}\left(\mathcal{S}(E) : E \in \mathcal{E}\right) := \frac{\displaystyle\sum_{E \in \mathcal{E}_{\mathcal{S}}} \omega_E^{-1}}{\displaystyle\sum_{E \in \mathcal{E}} \omega_E^{-1}}.$$

Using Birch's counting argument in [2, discussion after (1)] for the number of $E_{\alpha,\beta}$ in each equivalence class, Birch's result may be written as

$$\lim_{p \to \infty} \mathrm{Pr}_{\mathrm{Aut}}\left(a \leq x_E \leq b : E \in \mathcal{E}(p)\right) = \mu_{\mathrm{ST}}([a,b]).$$

It is well-known that the discrepancy between the weighted and unweighted probabilities goes to zero as $p \to \infty$. The corresponding relationship for the weighted and unweighted moments of traces in arithmetic progressions is given in the following lemma.

Lemma 2.5. *Let $m \in \mathbb{Z}$ and $M, r \in \mathbb{N}$. Then as $p \to \infty$ we have*

$$S_{\nu,m,M}(p^r) = 2^{\nu-1} p^{\frac{r\nu}{2}} \sum_{E \in \mathcal{E}_{m,M}(p^r)} x_E^{\nu} + O_{\nu}\left(p^{\frac{r\nu}{2}}\right). \tag{2.2}$$

Proof. First note that for $\nu \in \mathbb{N}_0$ we have

$$S_{\nu,m,M}(p^r) = 2^{\nu-1} p^{\frac{r\nu}{2}} \sum_{E \in \mathcal{E}_{m,M}(p^r)} x_E^{\nu} + 2^{\nu} p^{\frac{r\nu}{2}} \sum_{\substack{E \in \mathcal{E}_{m,M}(p^r) \\ \omega_E \neq 2}} \left(\frac{1}{\omega_E} - \frac{1}{2}\right) x_E^{\nu}. \tag{2.3}$$

It is well-known that the set of $E/\mathbb{F}_{p^r}$ with $\omega_E \neq 2$ is bounded by an absolute constant (see [24, Chapter III and Chapter X] for further details). Hence, as $p \to \infty$, by (2.3)

$$\left| \sum_{\substack{E \in \mathcal{E}_{m,M}(p^r) \\ \omega_E \neq 2}} \left(\frac{1}{\omega_E} - \frac{1}{2}\right) x_E^{\nu} \right| \leq \frac{1}{2} \#\{E/\mathbb{F}_{p^r} : \omega_E \neq 2\} \ll 1,$$

yielding the lemma. $\qquad \square$

3. Evaluation of the Rankin–Cohen brackets

As in [3, Lemma 2.6 (3)] (see also [18, (4.6)], where the Fourier expansion differs slightly), we have

$$[\mathcal{H}, \theta_{1,m,M}]_k = \pi_{\mathrm{hol}}\left(\left[\widehat{\mathcal{H}}, \theta_{1,m,M}\right]_k\right) - \pi_{\mathrm{hol}}\left(\left[\mathcal{H}^-, \theta_{1,m,M}\right]_k\right). \tag{3.1}$$

Writing

$$[\mathcal{H}, \theta_{1,m,M}]_k(\tau) = \sum_{n=0}^{\infty} c_{k,m,M}(n) q^n, \tag{3.2}$$

the idea is to obtain asymptotic behavior $c_{k,m,M}(n)$ by bounding the coefficients of the individual terms on the right-hand side of (3.1). We begin by considering the first term on the right-hand side of (3.1). We recall its modular properties, which leads to a bound by Deligne's work [7].

Lemma 3.1. *For $k \in \mathbb{N}_0$ we have*

$$\pi_{\mathrm{hol}}\left(\left[\widehat{\mathcal{H}}, \theta_{1,m,M}\right]_k\right) \in S_{2k+3}\left(\Gamma_{4M^2,M}\right).$$

Hence the n-th coefficient of $\pi_{\mathrm{hol}}([\widehat{\mathcal{H}}, \theta_{1,m,M}]_k)$ is $O(n^{k+1+\varepsilon})$.

Proof. From [18, Theorem 4.2], $\pi_{\mathrm{hol}}([\widehat{\mathcal{H}}, \theta_{1,m,M}]_k)$ is a modular form of weight $2k+3$ on $\Gamma_{4M^2,M}$. To see that this is a cusp form, we follow the same argument as given in [18] between [18, (7.2) and (7.3)]. Namely, since $\theta_{1,m,M}$ is a cusp form and holomorphic projection and the Rankin–Cohen bracket both commute with slashing, for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ we have

$$\pi_{\mathrm{hol}}\left(\left[\widehat{\mathcal{H}}, \theta_{1,m,M}\right]_k\right)\big|_{2k+3}\gamma = \pi_{\mathrm{hol}}\left(\left[\widehat{\mathcal{H}}\big|_{\frac{3}{2}}\gamma, \theta_{1,m,M}\big|_{\frac{3}{2}}\gamma\right]_k\right),$$

and the vanishing of the constant term of $\theta_{1,m,M}\big|_{\frac{3}{2}}\gamma$ implies that the holomorphic projection vanishes towards every cusp, and is hence a cusp form.

For the second claim, we use Deligne's bound [7] for cusp forms. $\qquad\square$

Using Lemma 3.1, we next relate $c_{k,m,M}(n)$ to

$$F_{k,t}(s) := 2^{-2k}\frac{2k+1}{2k+2}\binom{2k}{k}(t-s)^{2k+2}.$$

To state the result, we use $\sum_{s,t}^*$ to denote the sum over s and t where the term with $s = 0$ is weighted by $\frac{1}{2}$.

Lemma 3.2. *We have*

$$c_{k,m,M}(n) = -\frac{1}{2}\sum_{\substack{t^2-s^2=n \\ t\equiv\pm m \pmod M}}^* F_{k,t}(s) + O_{k,M}\left(n^{k+1+\varepsilon}\right).$$

Proof. Plugging Lemma 3.1 into (3.1), it remains to show that the n-th Fourier coefficient of $\pi_{\mathrm{hol}}\left([\mathcal{H}^-, \theta_{1,m,M}]_k\right)$ is

$$-\frac{1}{2}\sum_{\substack{t^2-s^2=n \\ t\equiv\pm m \pmod M}}^* F_{k,t}(s) + O_{k,M}\left(n^{k+1+\varepsilon}\right).$$

To do so, we separately consider the contribution from the (non-holomorphic) constant term of $\mathcal{H}^-$ and the remaining terms, starting with the constant term. Noting that the n-th Fourier coefficient of $\theta_{1,m,M}$ is

$$\begin{cases} n & \text{if } n = t^2 \text{ and } t \equiv m \pmod M \text{ with } -t \not\equiv m \pmod M, \\ 2n & \text{if } n = t^2 \text{ and } \pm t \equiv m \pmod M, \\ 0 & \text{otherwise,} \end{cases}$$

we plug in Lemma 2.1 (1) with $\kappa_1 = \kappa_2 = \frac{3}{2}$ and $g = \theta_{1,m,M}$ to evaluate

$$\pi_{\mathrm{hol}}\left(\left[\frac{1}{\sqrt{v}}, \theta_{1,m,M}\right]_k\right) = \alpha_{\frac{3}{2},\frac{3}{2},k}\sum_{n\equiv m \pmod M} t^{2k+2}q^{t^2}.$$

Hence the t^2-th coefficient is $O(n^{k+1})$.

9

It remains to evaluate the contribution from $\mathcal{H}_0^-(\tau) = \mathcal{H}^-(\tau) - \frac{1}{8\pi\sqrt{v}}$. We use Lemma 2.1 (2) with $\kappa_1 = \kappa_2 = \frac{3}{2}$, $F = \widehat{\mathcal{H}}$, and $g = \theta_{1,m,M}$. Writing $j = t^2$ and $\ell = s^2$ in the sum defining $b(n)$ in Lemma 2.1 (2), the sum runs over $t^2 - s^2 = n$ with $t \in \mathbb{N}$ satisfying $t \equiv \pm m \pmod{M}$ and $s \in \mathbb{N}$ (i.e., $n = (t+s)(t-s)$ and evaluating $\Gamma(-\frac{1}{2}) = -2\sqrt{\pi}$, the n-th Fourier coefficient of $\pi_{\mathrm{hol}}([\widehat{\mathcal{H}}_0^-, \theta_{1,m,M}]_k)$ equals

$$
2\sqrt{\pi} \sum_{\pm} \sum_{\substack{t^2-s^2=n \\ t\equiv \pm m \pmod{M}}} \sum_{\mu=0}^{k} \binom{k+\frac{1}{2}}{k-\mu}\binom{k+\frac{1}{2}}{\mu} t^{2k-2\mu+1} \frac{1}{4\sqrt{\pi}} \left(t^{2\mu-4k-1} P_{3+2k,\frac{1}{2}-\mu}\left(n, s^2\right) - s^{2\mu+1}\right)
$$

$$
= \frac{1}{2} \sum_{\substack{t^2-s^2=n \\ t\equiv \pm m \pmod{M}}} \sum_{\mu=0}^{k} \binom{k+\frac{1}{2}}{k-\mu}\binom{k+\frac{1}{2}}{\mu} t^{2k-2\mu+1} \left(t^{2\mu-4k-1} P_{2k+3,\frac{1}{2}-\mu}\left(n, s^2\right) - s^{2\mu+1}\right). \quad (3.3)
$$

By [22, Proposition 4.2], we have

$$
\sum_{\mu=0}^{k} \binom{k+\frac{1}{2}}{k-\mu}\binom{k+\frac{1}{2}}{\mu} t^{2k-2\mu+1} \left(t^{2\mu-4k-1} P_{2k+3,\frac{1}{2}-\mu}\left(n, s^2\right) - s^{2\mu+1}\right) = F_{k,t}(s),
$$

and thus (3.3) simplifies to give the claim. $\qquad\square$

We next use Lemma 3.2 to rewrite the asymptotics at $c_{\ell,m,M}(n)$ in terms of sums of divisors.

Proposition 3.3. *Let* $m \in \mathbb{Z}$, $M \in \mathbb{N}$, *and* $k \in \mathbb{N}_0$ *be given. Then, as* $n \to \infty$, *for any* $\varepsilon > 0$ *we have*

$$
c_{k,m,M}(n) = -2^{-2k-1}\frac{2k+1}{2k+2}\binom{2k}{k} \sum_{\substack{d|n, \ d^2 \leq n \\ d+\frac{n}{d}\equiv \pm 2m \pmod{2M}}}^{*} d^{2k+2} + O_{k,M,\varepsilon}\left(n^{k+1+\varepsilon}\right),
$$

where here $\sum^{*}$ *means the term with* $d = \sqrt{n}$ *(if it occurs) is counted with multiplicity* $\frac{1}{2}$.

Proof. By Lemma 3.2, we have

$$
c_{k,m,M}(n) = -2^{-2k-1}\frac{2k+1}{2k+2}\binom{2k}{k} \sum_{\substack{t^2-s^2=n \\ t\equiv \pm m \pmod{M}}}^{*} (t-s)^{2k+2} + O_{k,M}\left(n^{k+1+\varepsilon}\right).
$$

We now write $t - s = d$ and $t + s = \frac{n}{d} \geq d$ (using $s \geq 0$). Note that there is a bijection between pairs (t,s) and $d \mid n$ with $d^2 \leq n$ satisfying the congruence $d + \frac{n}{d} \equiv \pm 2m \pmod{2M}$ because $2t = d + \frac{n}{d}$ and $2s = \frac{n}{d} - d$ are uniquely determined from d. Using $d + \frac{n}{d} = 2t$, this gives the claim. $\qquad\square$

4. Proof of Theorem 1.4

Recalling (3.2), we write

$$
[\mathcal{H}, \theta_{1,m,M}]_k \,|U_4(\tau) = \frac{1}{(2\pi i)^k} \sum_{j=0}^{k} d_{k,j}\left(\mathcal{H}^{(j)}\theta_{1,m,M}^{(k-j)}\right)|U_4(\tau) = \sum_{n=0}^{\infty} c_{k,m,M}(4n) q^n,
$$

where

$$
d_{k,j} := (-1)^j \binom{k+\frac{1}{2}}{j}\binom{k+\frac{1}{2}}{k-j}
$$

10

are the coefficients from the Rankin–Cohen brackets. We next solve for $H_{2\ell+1,m,M}(n)$ in terms of $c_{k,m,M}(4n)$ and $H_{2k-2\ell+1,m,M}(n)$ with $\ell > 0$. For this, define

$$\mathcal{C}_k := \sum_{j=0}^{k} (-1)^j d_{k,j}.$$

A straightforward calculation shows the following.

Lemma 4.1. *We have*

$$H_{2k+1,m,M}(n) = \frac{1}{\mathcal{C}_k} c_{k,m,M}(4n) - \frac{1}{\mathcal{C}_k} \sum_{j=1}^{k} d_{k,j} \sum_{\ell=1}^{j} (-1)^{j+\ell} \binom{j}{\ell} (4n)^{\ell} H_{2k-2\ell+1,m,M}(n).$$

We next bound $c_{k,m,M}(4n)$.

Lemma 4.2. *Let $k \in \mathbb{N}_0$, $m \in \mathbb{Z}$, and $M \in \mathbb{N}$. Then we have, as $n \to \infty$,*

$$c_{k,m,M}(4n) \ll_{k,M} n^{k+1+\varepsilon}.$$

Proof. By Proposition 3.3, we have

$$c_{k,m,M}(4n) = -2^{-2k-1} \frac{2k+1}{2k+2} \binom{2k}{k} \sum_{\substack{d|4n,\ d^2 \le 4n \\ d+\frac{4n}{d} \equiv \pm 2m \pmod{2M}}}^{*} d^{2k+2} + O_{k,M,\varepsilon}\left(n^{k+1+\varepsilon}\right).$$

Since $d^2 \le 4n$, we have

$$d^{2k+2} \le 4^{k+1} n^{k+1},$$

so (noting that $d \mid 4n$ and $\sigma_0(n) \ll_\varepsilon n^\varepsilon$ as $n \to \infty$, where $\sigma_r(n) := \sum_{d|n} d^r$)

$$c_{k,m,M}(4n) \ll_{k,M} n^{k+1} \sigma_0(4n) + n^{k+1+\varepsilon} \ll_{k,M} n^{k+1+\varepsilon}. \qquad \square$$

We are now ready to prove Theorem 1.4.

Proof of Theorem 1.4. By [3, Lemma 3.7], we have

$$H_{m,M}(n) \gg_\varepsilon n^{1-\varepsilon}.$$

Thus if

$$H_{2k+1,m,M}(n) = O_{k,M,\varepsilon}\left(n^{k+1+\varepsilon}\right), \tag{4.1}$$

then

$$\frac{H_{2k+1,m,M}(n)}{n^{k+\frac{1}{2}} H_{m,M}(n)} = O_{k,M,\varepsilon}\left(n^{-\frac{1}{2}+\varepsilon}\right).$$

It hence suffices to show (4.1). We prove (4.1) by induction. For $k = 0$, Lemma 4.1 followed by Lemma 4.2 implies that

$$H_{1,m,M}(n) = \frac{1}{\mathcal{C}_1} c_{1,m,M}(4n) \ll_{k,M} n^{2+\varepsilon}.$$

This gives the claim for $k = 0$. We next assume the claim for $1 \le j < k$ and use Lemma 4.1. Together with Lemma 4.2 and the inductive hypothesis, this gives the claim. $\qquad \square$

11

5. Proof of Theorem 1.3

We first recall that by [3, Lemma 2.2], we have

$$2S_{\nu,m,M}(p^r) = H_{\nu,m,M}(p^r) + E_{\nu,m,M}(p^r), \tag{5.1}$$

where

$$E_{\nu,m,M}(p^r) := \delta_{M|m}\delta_{\nu=0}\delta_{2\nmid r}H(4p) + \delta_{M|m}\delta_{\nu=0}\delta_{2|r}\frac{1}{2}\left(1 - \left(\frac{-1}{p}\right)\right)$$
$$+ \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right)p^{\frac{\nu r}{2}}\varrho_{\nu,m,M}(p^r) + \frac{1}{3}(p-1)2^{\nu-2}p^{\frac{\nu r}{2}}\sigma_{\nu,m,M}(p^r)$$

with

$$\varrho_{\nu,m,M}(p^r) := \sum_{\substack{t\equiv m \pmod M \\ t^2=p^r}} \mathrm{sgn}(t)^\nu, \qquad \sigma_{\nu,m,M}(p^r) := \sum_{\substack{t\equiv m \pmod M \\ t^2=4p^r}} \mathrm{sgn}(t)^\nu.$$

Analogous to [3, Lemma 4.2], we require a bound for $E_{2k+1,m,M}(p^r)$ with $k \in \mathbb{N}_0$.

Lemma 5.1. *For $k \in \mathbb{N}_0$ and $r \in \mathbb{N}$, we have*

$$E_{2k+1,m,M}(p^r) = \frac{2^{2k-1}}{3}p^{\left(k+\frac{1}{2}\right)r+1}\sigma_{2k+1,m,M}(p^r) + O_k\left(p^{\left(k+\frac{1}{2}\right)r}\right).$$

Moreover,

$$E_{2k+1,m,M}(p^r) = O_k\left(p^{\left(k+\frac{1+\delta_{2|r}}{2}\right)r}\right).$$

Proof. The first two terms in the definition of $E_{2k+1,m,M}(p^r)$ vanish because $2k+1 > 0$ by assumption. We then note that

$$|\varrho_{\nu,m,M}(p^r)| \leq \sum_{\substack{t\equiv m \pmod M \\ t^2=p^r}} |\mathrm{sgn}(t)^\nu| \leq \sum_{\substack{t\equiv m \pmod M \\ t^2=p^r}} 1 \leq 2, \tag{5.2}$$

$$|\sigma_{\nu,m,M}(p^r)| \leq \sum_{\substack{t\equiv m \pmod M \\ t^2=4p^r}} |\mathrm{sgn}(t)^\nu| = \sum_{\substack{t\equiv m \pmod M \\ t^2=4p^r}} 1 \leq 2. \tag{5.3}$$

From (5.2), the third term in the definition of $E_{2k+1,m,M}(p^r)$ is $O(p^{(k+\frac{1}{2})r})$. For the final term, we split the factor $p-1$ into two terms, with p giving the main term and -1 giving $O_k(p^{(k+\frac{1}{2})r})$ by (5.3). This yields the first claim.

If r is odd, then $t^2 = 4p^r$ is not solvable, thus $\sigma_{2k+1,m,M}(p^r) = 0$, giving the second claim. For r even, we have $r \geq 2$, so by (5.3)

$$\frac{2^{2k-1}}{3}p^{\left(k+\frac{1}{2}\right)r+1}\sigma_{2k+1,m,M}(p^r) \ll_k p^{\left(k+\frac{1}{2}\right)r+\frac{r}{2}} = O_k\left(p^{(k+1)r}\right),$$

as claimed. $\qquad\square$

We are now ready to prove Theorem 1.3.

Proof of Theorem 1.3. Plugging Lemma 5.1 into (5.1), we have

$$S_{2k+1,m,M}(p^r) = \frac{1}{2}H_{2k+1,m,M}(p^r) + O_k\left(p^{(k+1)r}\right).$$

We then plug in Theorem 1.4 to obtain

$$S_{2k+1,m,M}(p^r) = O_{k,M,\varepsilon}\left(p^{(k+1+\varepsilon)r}\right). \qquad\square$$

12

6. Proof of Theorems 1.1 and 1.2

In this section, we consider the implications of Theorem 1.3 to the study of distributions of the trace of Frobenius.

To prove that the weighted averages of x_E for $E/\mathbb{F}_p$ are equidistributed with respect to the Sato–Tate measure as $p \to \infty$, Birch [2] computed the moments as

$$\sum_{E/\mathbb{F}_p} \frac{\mathrm{tr}(E)^{2k}}{\omega_E} \sim C_k p^k.$$

Up to a normalization factor, these match the moments in Lemma 2.4. Following Birch's argument, we are now ready to prove the following weighted version of Theorem 1.1.

Theorem 6.1. *Let $m \in \mathbb{Z}$ and $M, r \in \mathbb{N}$ be given. The set $\{x_E : E \in \mathcal{E}_{m,M}(p^r)\}$ becomes equidistributed with respect to the Sato–Tate measure as $p \to \infty$. Specifically, we have*

$$\lim_{p \to \infty} \mathrm{Pr}_{\mathrm{Aut}}\left(a \le x_E \le b : E \in \mathcal{E}_{m,M}(p^r)\right) = \mu_{\mathrm{ST}}([a,b]).$$

Proof. By (1.3), for $\nu \in \mathbb{N}_0$, the ν-th weighted moment with respect to x_E for $E \in \mathcal{E}_{m,M}(p^r)$ is

$$\mu_\nu(p^r) := \frac{1}{S_{m,M}(p^r)} \sum_{E \in \mathcal{E}_{m,M}(p^r)} \frac{x_E^\nu}{\omega_E} = \frac{S_{\nu,m,M}(p^r)}{2^\nu p^{\frac{r\nu}{2}} S_{m,M}(p^r)}. \tag{6.1}$$

If ν is odd, then Theorem 1.3 implies that (see (1.6) in particular)

$$\lim_{p \to \infty} \mu_\nu(p^r) = 0. \tag{6.2}$$

If $\nu = 2k$ is even, then we plug in (1.5) to obtain

$$\lim_{p \to \infty} \mu_\nu(p^r) = \frac{C_k}{2^{2k}}. \tag{6.3}$$

Comparing (6.2) and (6.3) with Lemma 2.4, we conclude that

$$\lim_{p \to \infty} \mu_\nu(p^r) = \delta_{2|\nu} \frac{C_{\frac{\nu}{2}}}{2^\nu} = \mu_{\mathrm{ST},\nu}. \tag{6.4}$$

Since the moments $\mu_\nu(p^r)$ converge to $\mu_{\mathrm{ST},\nu}$ and the distribution is uniquely determined by its moments [1, Theorem 30.1 and Theorem 30.2] (as pointed out by Birch [2], the Sato–Tate distribution satisfies the necessary conditions), we conclude that

$$\lim_{p \to \infty} \mathrm{Pr}_{\mathrm{Aut}}\left(a \le x_E \le b : E \in \mathcal{E}_{m,M}(p^r)\right) = \mu_{\mathrm{ST}}([a,b]). \qquad \square$$

We now compare the weighted and unweighted distributions in order to obtain Theorem 1.1.

Proof of Theorem 1.1. Since we take $p \to \infty$, we may assume that $p \ge 5$. In order to obtain the claim, we need to show that

$$\lim_{p \to \infty} \frac{1}{\#\mathcal{E}_{m,M}(p^r)} \sum_{E \in \mathcal{E}_{m,M}(p^r)} x_E^\nu = \mu_{\mathrm{ST},\nu}. \tag{6.5}$$

By (6.4) (plugging in (6.1) to the left-hand side), we have

$$\lim_{p \to \infty} \frac{S_{\nu,m,M}(p^r)}{2^\nu p^{\frac{r\nu}{2}} S_{m,M}(p^r)} = \mu_{\mathrm{ST},\nu}. \tag{6.6}$$

Using Lemma 2.5 and then (1.7), we have

$$\frac{S_{\nu,m,M}(p^r)}{2^\nu p^{\frac{r\nu}{2}} S_{m,M}(p^r)} = \frac{\frac{1}{2} \sum_{E \in \mathcal{E}_{m,M}(p^r)} x_E^\nu}{S_{m,M}(p^r)} + O_{\nu,M,\varepsilon}\left(p^{(\varepsilon-1)r}\right).$$

13

In the main term, we use Lemma 2.5 and note that $\sum_{E\in\mathcal{E}_{m,M}(p^r)} 1 = \#\mathcal{E}_{m,M}(p^r)$ to rewrite

$$S_{m,M}(p^r) = \frac{1}{2}\#\mathcal{E}_{m,M}(p^r) + O(1). \tag{6.7}$$

Using (1.7), we see that have $\#\mathcal{E}_{m,M}(p^r) \gg_{M,\varepsilon} p^{(1-\varepsilon)r}$ and hence

$$\frac{S_{\nu,m,M}(p^r)}{2^\nu p^{\frac{r\nu}{2}} S_{m,M}(p^r)} = \frac{\frac{1}{2}\sum_{E\in\mathcal{E}_{m,M}(p^r)} x_E^\nu}{\frac{1}{2}\#\mathcal{E}_{m,M}(p^r) + O(1)} + O_{\nu,M,\varepsilon}\left(p^{(\varepsilon-1)r}\right)$$

$$= \frac{\frac{1}{2}\sum_{E\in\mathcal{E}_{m,M}(p^r)} x_E^\nu}{\frac{1}{2}\#\mathcal{E}_{m,M}(p^r)\left(1 + O_{M,\varepsilon}\left(p^{(\varepsilon-1)r}\right)\right)} + O_{\nu,M,\varepsilon}\left(p^{(\varepsilon-1)r}\right). \tag{6.8}$$

Expanding the geometric series, we have

$$\frac{\frac{1}{2}\sum_{E\in\mathcal{E}_{m,M}(p^r)} x_E^\nu}{\frac{1}{2}\#\mathcal{E}_{m,M}(p^r)\left(1 + O_{M,\varepsilon}\left(p^{(\varepsilon-1)r}\right)\right)} = \frac{\frac{1}{2}\sum_{E\in\mathcal{E}_{m,M}(p^r)} x_E^\nu}{\frac{1}{2}\#\mathcal{E}_{m,M}(p^r)}\left(1 + O_{M,\varepsilon}\left(p^{(\varepsilon-1)r}\right)\right)$$

$$= \frac{\sum_{E\in\mathcal{E}_{m,M}(p^r)} x_E^\nu}{\#\mathcal{E}_{m,M}(p^r)} + O_{M,\varepsilon}\left(p^{(\varepsilon-1)r}\right),$$

where in the last step we use the fact that $|\sum_{E\in\mathcal{E}_{m,M}(p^r)} x_E^\nu| \leq \#\mathcal{E}_{m,M}(p^r)$. Plugging back into (6.8) and rearranging, we obtain that

$$\frac{\sum_{E\in\mathcal{E}_{m,M}(p^r)} x_E^\nu}{\#\mathcal{E}_{m,M}(p^r)} = \frac{S_{\nu,m,M}(p^r)}{2^\nu p^{\frac{r\nu}{2}} S_{m,M}(p^r)} + O_{\nu,M,\varepsilon}\left(p^{(\varepsilon-1)r}\right). \tag{6.9}$$

Thus by (6.6) we have

$$\lim_{p\to\infty} \frac{\sum_{E\in\mathcal{E}_{m,M}(p^r)} x_E^\nu}{\#\mathcal{E}_{m,M}(p^r)} = \mu_{\mathrm{ST},\nu}. \qquad \square$$

By restricting the sample space to $\mathcal{E}_{m,M}$, Theorem 6.1 investigates the (weighted) conditional probability that the normalized traces lie in a given interval under the assumption that $E \in \mathcal{E}_{m,M}(p^r)$. It is also interesting to consider the distribution of normalized traces x_E from $E \in \mathcal{E}_{m,M}$ within the larger sample space $\mathcal{E}(p^r)$. Equivalently, weighting the probabilities via the reciprocal of the size of the automorphism group as before, we consider the moments

$$\frac{\sum_{\substack{E/\mathbb{F}_p \\ \mathrm{tr}(E)\equiv m \pmod{M}}} \frac{x_E^\nu}{\omega_E}}{S_{1,1}(p)} = \frac{\frac{1}{2^\nu}\sum_{\substack{E/\mathbb{F}_p \\ \mathrm{tr}(E)\equiv m \pmod{M}}} \frac{\mathrm{tr}(E)^\nu}{\omega_E}}{p^{\frac{\nu}{2}} S_{1,1}(p)}$$

$$= \frac{\frac{1}{2^\nu}\sum_{\substack{E/\mathbb{F}_p \\ \mathrm{tr}(E)\equiv m \pmod{M}}} \frac{\mathrm{tr}(E)^\nu}{\omega_E}}{p^{\frac{\nu}{2}} S_{m,M}(p)} \frac{S_{m,M}(p)}{S_{1,1}(p)} \tag{6.10}$$

as $p \to \infty$. Since the limit of the first factor in (6.10) exists by (6.4), the limit as $p \to \infty$ of the the above distribution exists if and only if

$$\lim_{p\to\infty} \frac{S_{m,M}(p)}{S_{1,1}(p)}$$

exists. The closely-related limits (1.2) were computed in [5, Theorem 1], where the authors gave a full description of the distribution, so one may obtain the asymptotic behavior by combining Theorem 6.1 with [5]. We restrict ourselves to certain cases where the above limit exists in order to get fixed multiples of the Sato–Tate distribution in the limit. In order to further relate the results in [5, Theorem 1] with the approach used here, we next describe how to determine the

14

limits considered in [5] via our method. For this, fix p to lie in a given congruence class modulo M. For $j \in \mathbb{N}$ with $\gcd(j, 2M) = 1$, we therefore set

$$c_{j,m,M} := \lim_{\substack{p \to \infty \\ p \equiv j \pmod{4M^2}}} \frac{S_{m,M}(p)}{S_{1,1}(p)}.$$

We reprove the conclusion of [5, Theorem 1] that these limits all exist.

Proposition 6.2. *For $m \in \mathbb{Z}$, $M \in \mathbb{N}$, and $j \in \mathbb{N}$ with $\gcd(j, 2M) = 1$, the limit $c_{j,m,M}$ exists.*

Remark. The limits are not in general independent of j, so the overall limit over all p does not (in general) exist.

Before proving Proposition 6.2, we conclude a weighted version of Theorem 1.2.

Theorem 6.3. *Let $m \in \mathbb{Z}$ and $M \in \mathbb{N}$. Then for each $j \in \mathbb{Z}$ with $\gcd(j, 2M) = 1$ there exists a constant $c_{j,m,M}$ such that for $-1 \le a \le b \le 1$ we have*

$$\lim_{\substack{p \to \infty \\ p \equiv j \pmod{4M^2}}} \mathrm{Pr}_{\mathrm{Aut}} \left(a \le x_E \le b \text{ and } E \in \mathcal{E}_{m,M}(p) : E \in \mathcal{E}(p) \right) = c_{j,m,M} \mu_{\mathrm{ST}}([a, b]).$$

Proof. Plugging Proposition 6.2 and (6.4) into (6.10), we obtain

$$\lim_{\substack{p \to \infty \\ p \equiv j \pmod{4M^2}}} \frac{\displaystyle\sum_{\substack{E/\mathbb{F}_p \\ \mathrm{tr}(E) \equiv m \pmod{M}}} \frac{x_E^\nu}{\omega_E}}{S_{1,1}(p)} = \begin{cases} c_{j,m,M} \frac{C_k}{2^{2k}} & \text{if } \nu = 2k \text{ is even,} \\ 0 & \text{if } \nu \text{ is odd.} \end{cases}$$

By Lemma 2.4, this matches the ν-th moment of $c_{j,m,M}$ times the Sato–Tate measure. Since the distribution is uniquely determined by its moments, as in [1, Theorem 30.1 and Theorem 30.2],

$$\lim_{\substack{p \to \infty \\ p \equiv j \pmod{4M^2}}} \mathrm{Pr}_{\mathrm{Aut}} \left(a \le x_E \le b \text{ and } E \in \mathcal{E}_{m,M}(p) : E \in \mathcal{E}(p) \right) = c_{j,m,M} \mu_{\mathrm{ST}}([a, b]).$$

Hence for $E \in \mathcal{E}_{m,M}(p)$ within the larger space $\mathcal{E}(p)$, we see that x_E is equidistributed in $[-1, 1]$ with respect to $c_{j,m,M}$ times the Sato–Tate measure as $p \to \infty$ with $p \equiv j \pmod{4M^2}$. This gives the claim. $\qquad\square$

We next show how to conclude Theorem 6.3 from Theorem 1.2.

Proof of Theorem 1.2. Since the ν-th moment of $c\mu_{\mathrm{ST}}$ is $c\mu_{\mathrm{ST},\nu}$ for $c \in \mathbb{R}$, the claim is equivalent to showing that

$$\lim_{\substack{p \to \infty \\ p \equiv j \pmod{4M^2}}} \frac{1}{\#\mathcal{E}(p)} \sum_{E \in \mathcal{E}_{m,M}(p)} x_E^\nu = c_{j,m,M} \mu_{\mathrm{ST},\nu}. \tag{6.11}$$

By (6.5), we have

$$\lim_{p \to \infty} \frac{1}{\#\mathcal{E}_{m,M}(p)} \sum_{E \in \mathcal{E}_{m,M}(p)} x_E^\nu = \mu_{\mathrm{ST},\nu}.$$

Thus (6.11) is equivalent to

$$\lim_{\substack{p \to \infty \\ p \equiv j \pmod{4M^2}}} \frac{\#\mathcal{E}_{m,M}(p)}{\#\mathcal{E}(p)} = c_{j,m,M}. \tag{6.12}$$

To show (6.12), we use (6.7) to rewrite

$$\frac{\#\mathcal{E}_{m,M}(p)}{\#\mathcal{E}(p)} = \frac{S_{m,M}(p) + O(1)}{S_{1,1}(p) + O(1)}.$$

15

We then plug in (1.7) to obtain

$$\frac{S_{m,M}(p) + O(1)}{S_{1,1}(p) + O(1)} = \frac{S_{m,M}(p)}{S_{1,1}(p)} \frac{1 + O_{M,\varepsilon}\left(p^{\varepsilon-1}\right)}{1 + O_\varepsilon\left(p^{\varepsilon-1}\right)} = \frac{S_{m,M}(p)}{S_{1,1}(p)}\left(1 + O_{M,\varepsilon}\left(p^{\varepsilon-1}\right)\right).$$

By Proposition 6.2, if $p \equiv j \pmod{4M^2}$, then the right-hand side becomes

$$c_{j,m,M}\left(1 + o_M(1)\right),$$

yielding (6.12), and hence the claim. $\square$

We finally prove Proposition 6.2.

Proof of Proposition 6.2. We claim that there exist constants $a_{j,m,M} > 0$ and $b_{j,m,M} \in \mathbb{C}$ only depending on j, m, M such that for $p \equiv j \pmod{4M^2}$ we have

$$S_{m,M}(p) = a_{j,m,M}p + b_{j,m,M} + O_{m,M}\left(p^{\frac{1}{2}+\varepsilon}\right) = a_{j,m,M}p + O_{j,m,M}\left(p^{\frac{1}{2}+\varepsilon}\right). \qquad (6.13)$$

Assuming (6.13), for $p \equiv j \pmod{4M^2}$ we have

$$\frac{S_{m,M}(p)}{S_{1,1}(p)} = \frac{a_{j,m,M}p + O_{j,m,M}\left(p^{\frac{1}{2}+\varepsilon}\right)}{a_{j,1,1}p + O_{j,m,M}\left(p^{\frac{1}{2}+\varepsilon}\right)} = \frac{a_{j,m,M}}{a_{j,1,1}} + O_{j,m,M}\left(p^{-\frac{1}{2}+\varepsilon}\right),$$

thus

$$\lim_{\substack{p \to \infty \\ p \equiv j \pmod{M}}} \frac{S_{m,M}(p)}{S_{1,1}(p)} = \frac{a_{j,m,M}}{a_{j,1,1}} =: s_{j,m,M}.$$

It therefore remains to prove (6.13). Plugging [3, Lemma 4.2] (note that $\varrho_{m,M}(p) = 0$ because p is not a square) into (5.1) yields

$$S_{m,M}(p) = \frac{1}{2}H_{m,M}(p) + O\left(p^{\frac{1}{2}+\varepsilon}\right).$$

This reduces (6.13) to showing the same claim for $H_{m,M}(p)$. By [3, Lemma 3.2], we have $H_{m,M}(p) = G_{m,M}(p)$ and $G_{m,M}(p)$ is the p-th coefficient of $2\left[\mathcal{H}, \theta_{m,M}\right]_0$ by [3, Lemma 3.1]. By [3, Lemma 3.3], we have that

$$f := \left(2\left[\mathcal{H}, \theta_{m,M}\right] + \Lambda_{1,m,M}\right)\big|U_4$$

is a weight two quasimodular form on $\Gamma_{4M^2,M}$. The n-th coefficient of $\Lambda_{1,m,M}|U_4$ is $O_{m,M}(n^{\frac{1}{2}+\varepsilon})$ because $t^2 - s^2 = 4n$ implies that $t - s \le 2\sqrt{n}$.

Thus it remains to show that the p-th coefficient of f has the desired shape. We write

$$f = E + g$$

where g is a cusp form and E is in the space spanned by Eisenstein series (which are spanned by E_2 and holomorphic modular forms that are orthogonal to cusp forms) Using the bound of Deligne [7], the p-th coefficient of g is bounded by $O(p^{\frac{1}{2}+\varepsilon})$. To compute the p-th coefficient of E, we use a basis given by E_2 and a basis for the space of holomorphic Eisenstein series of weight two. We first note that, by [21, (1.7)],

$$M_2\left(\Gamma_{4M^2,M}\right) \subseteq M_2\left(\Gamma_1\left(4M^2\right)\right) \cong \bigoplus_\chi M_2\left(\Gamma_0\left(4M^2\right), \chi\right),$$

where χ runs over characters modulo $4M^2$. A basis for the space of Eisenstein series in $M_2(\Gamma_0(4M^2), \chi)$ may be found in [8, Theorem 4.6.2]. These are enumerated by pairs of characters ψ and φ modulo $4M^2$ for which $\psi\varphi = \chi$ and $t \in \mathbb{N}$ such that $c(\psi)c(\varphi)t \mid 4M^2$, where $c(\psi)$ is the conductor. Writing $E_{2,\psi,\varphi,t}$ for the corresponding Eisenstein series, there exists constants $\lambda_{\psi,\varphi,t}$ such

16

that (note that in [8, Theorem 4.6.2], the case $(\psi, \varphi, 1)$ is omitted, but this precisely corresponds to a multiple of E_2, so this is included for our quasimodular Eisenstein series)

$$E = \sum_{\psi,\varphi \ (\mathrm{mod}\ 4M^2)} \sum_{t \mid \frac{4M^2}{c(\psi)c(\varphi)}} \lambda_{\psi,\varphi,t} E_{2,\psi,\varphi,t}. \tag{6.14}$$

If either ψ or φ is non-trivial, then the n-th Fourier coefficient of $E_{2,\psi,\varphi,1}$ is given by $\sigma_{1,\psi,\varphi}(n)$, where

$$\sigma_{k,\psi,\varphi}(n) := \sum_{d \mid n} \varphi(d)\psi\left(\frac{n}{d}\right) d^k$$

and $E_{2,\psi,\varphi,t} := E_{2,\psi,\varphi,1}\big|V_t$. Since p is coprime to $4M^2$, for $\psi\varphi$ non-trivial only those with $t = 1$ may contribute to the sum. Since p is prime, the sum has at most two summands. Moreover, since $p \equiv j \pmod{4M^2}$ and φ and χ are characters modulo $4M^2$, we have

$$\sigma_{1,\psi,\varphi}(p) = \varphi(p)p + \psi(p) = \varphi(j)p + \psi(j).$$

For ψ and φ both trivial and $t \neq 1$, we have that

$$E_{2,1,1,t} := E_2 - tE_2\big|V_t.$$

while $E_{2,1,1,1} := E_2$. Again using the fact that p and $4M^2$ are coprime, the p-th coefficient of $E_{2,1,1,t}$ is $-24(p+1)$. Plugging into (6.14), for $p \equiv j \pmod{4M^2}$, the p-th Fourier coefficient of E is

$$\sum_{\substack{\psi,\varphi \ (\mathrm{mod}\ 4M^2) \\ (\psi,\varphi)\neq(1,1)}} \sum_{t \mid \frac{4M^2}{c(\psi)c(\varphi)}} \lambda_{\psi,\varphi,t} \left(\varphi(j)p + \psi(j)\right) - 24 \sum_{t \mid 4M^2} \lambda_{1,1,t}(p+1)$$

$$= \left(\sum_{\substack{\psi,\varphi \ (\mathrm{mod}\ 4M^2) \\ (\psi,\varphi)\neq(1,1)}} \sum_{t \mid \frac{4M^2}{c(\psi)c(\varphi)}} \lambda_{\psi,\varphi,t}\varphi(j) - 24 \sum_{t \mid 4M^2} \lambda_{1,1,t} \right) p$$

$$+ \sum_{\substack{\psi,\varphi \ (\mathrm{mod}\ 4M^2) \\ (\psi,\varphi)\neq(1,1)}} \sum_{t \mid \frac{4M^2}{c(\psi)c(\varphi)}} \lambda_{\psi,\varphi,t}\psi(j) - 24 \sum_{t \mid 4M^2} \lambda_{1,1,t}.$$

The two sums only depend on m, M, and j, yielding the claim. $\square$

REFERENCES

[1] P. Billingsley, *Probability and measure*, Wiley, New York, 1979.

[2] B. Birch, *How the number of points of an elliptic curve over a fixed prime field varies,* J. London Math. Soc. **43** (1968), 57–60.

[3] K. Bringmann, B. Kane, and S. Pujahari, *Distribution of moments of trace of Frobenius in arithmetic progressions and holomorphic projection,* submitted for publication.

[4] B. Brock and A. Granville, *More points than expected on curves over finite field extensions,* Finite Fields and Appl. **7** (2001), 70–91.

[5] W. Castryck and H. Hubrechts, *The distribution of the number of points modulo an integer on elliptic curves oover finite fields,* Ramanujan J. **30** (2013), 223–242.

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

[7] P. Deligne, *La conjecture de Weil I,* Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307.

[8] F. Diamond and J. Shurman, *A first course in modular forms,* Springer, 2005.

[9] B. Gross, D. Zagier, *Heegner points and derivatives of L-series,* Invent. Math. **84** (1986), 225–320.

[10] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper. I, II, and III,* J. reine angew. Math. **175** (1936), 55–62, 69–88, 193–208.

[11] F. Hirzebruch and D. Zagier, *Intersection numbers of curves on Hilbert modular surfaces and modular forms of Nebentypus*, Invent. Math. **36** (1976), 57–113.

[12] E. Howe, *On the group orders of elliptic curves over finite fields*, Compositio Math. **85** (1993), 229–247.

[13] N. Kaplan and I. Petrow, *Elliptic curves over a finite field and the trace formula*, Proc. London Math. Soc. **115** (2017), 1317–1372.

[14] N. Kaplan and I. Petrow, *Traces of Hecke operators and refined weight enumerators of Reed-Solomon codes*, Trans. Amer. Math. Soc. **370** (2018), 2537–2561.

[15] N. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, AMS Coll. Publ. **45**, AMS Math. Soc. , Providence, 1999.

[16] N. Koblitz, *Introduction to elliptic curves and modular forms*, Graduate texts in Math. **97**, Springer-Verlag, 1993.

[17] H. Lenstra, Jr. *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), 649–673.

[18] M. Mertens, *Eichler-Selberg type identities for mixed mock modular forms*, Adv. Math. **301** (2016), 359–382.

[19] M. Mertens, K. Ono, and L. Rolen, *Mock Modular Eisenstein series with Nebentypus*, Int. J. Number Theory **17** (2021), 683–697.

[20] M. Murty and N. Prabhu, *The error term in the Sato-tate theorem of Birch*, Bull. Aust. Math. Soc. **100**, 27–33.

[21] K. Ono, *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, CMBS Regional Conference Series in Mathematics **102** (2004), American Mathematical Society, Providence, RI, USA.

[22] K. Ono, H. Saad, and N. Saikia, *Distribution of values of Gaussian hypergeometric functions*, preprint, arxiv:2108.09560.

[23] G. Shimura, *On modular forms of half integral weight*, Ann. Math. **97** (1973), 440–481.

[24] J. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math. **106**, Second edition, Springer-Verlag, 2009.

[25] J. Sturm, *Projections of C^∞ automorphic forms,* Bull. Amer. Math. Soc. **2** (1980), 435–439.

UNIVERSITY OF COLOGNE, DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, WEYERTAL 86-90, 50931 COLOGNE, GERMANY

Email address: `kbringma@math.uni-koeln.de`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HONG KONG, POKFULAM, HONG KONG

Email address: `bkane@hku.hk`

INSTITUTE OF MATHEMATICS, WARSAW UNIVERSITY, BANACHA 2, 02-97 WARSAW, POLAND.
SCHOOL OF MATHEMATICAL SCIENCES, NATIONAL INSTITUTE OF SCIENCE EDUCATION AND RESEARCH, BHUBANESWAR, HBNI, P. O. JATNI, KHURDA 752050, ODISHA, INDIA

Email address: `spujahari@mimuw.edu.pl/spujahari@gmail.com`