Rend. Sem. Mat. Univ. Politec. Torino
Vol. 68, 4 (2010), 337 – 348

S. J. Miller*, M. Ram Murty and F. Strauch**

A COMBINATORIAL IDENTITY FOR STUDYING SATO–TATE TYPE PROBLEMS

Abstract. We derive a combinatorial identity which is useful in studying the distribution of Fourier coefficients of L-functions by allowing us to pass from knowledge of moments of the coefficients to the distribution of the coefficients.

1. Introduction

Recently M. Ram Murty and K. Sinha [7] proved effective equidistribution results showing the eigenvalues of Hecke operators on the space of cusp forms of weight k and level N agree with the Sato–Tate distribution. Their proof relied on bounding the discrepancy through an application of the Erdös–Turan inequality and estimates of exponential sums. In [6] the first two authors generalized their techniques to the Fourier coefficients of families of elliptic curves. The purpose of this note is to describe an interesting combinatorial identity needed in that analysis.

We first describe the problem that motivated this work. Recall that if

$$E : y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{Z}$ is an elliptic curve over $\mathbb{Q}$, the associated L-function is

$$L(E,s) \;=\; \sum_{n=1}^{\infty} \frac{a_E(n)}{n^s} \;=\; \prod_p \left(1 - \frac{a_E(p)}{p^s} + \frac{\chi_0(p)}{p^{2s-1}}\right)^{-1}, \tag{1}$$

with $\Delta = -16(4a^3 + 27b^2)$ the discriminant of E, χ_0 the principal character modulo Δ, and

$$\begin{aligned} a_E(p) &= p - \#\{(x,y) \in (\mathbb{Z}/p\mathbb{Z})^2 : y^2 \equiv x^3 + ax + b \bmod p\} \\ &= -\sum_{x \bmod p} \left(\frac{x^3 + ax + b}{p}\right). \end{aligned} \tag{2}$$

By Hasse's bound we know $|a_E(p)| \le 2\sqrt{p}$, so we may write $a_E(p) = 2\sqrt{p}\cos\theta_E(p)$, where we may choose $\theta_E(p) \in [0,\pi]$. The distribution of the $a_E(p)$'s is related to numerous problems of interest; for example, by the Birch and Swinnerton–Dyer conjecture the order of vanishing of $L(E,s)$ at the central point $s = 1/2$ is conjecturally equal to the group of rational solutions of E. See [16, 17, 18] for more on elliptic curves.

*Partially supported by NSF grant DMS0970067.
**Partially supported by an NSERC Discovery grant.

In the analysis in [6], one needs to understand sums of $\cos(m\theta_n)$, with n ranging over a family of L-functions. Such estimates exist [3, 4, 8], and have been used by others to prove effective equidistribution results for two-parameter families of elliptic curves [1, 14, 15]. It is possible to avoid these estimates if instead one uses results of Birch [2] for sums of the moments, i.e. sums of $\cos^r(\theta_n)$. While typically these lead to worse results, as there may be situations in future research where only the moments are known, we describe how one may prove effective equidistribution results concerning the distribution of the Fourier coefficients of L-functions using just the moments and combinatorics.

The key combinatorial ingredient in [6] is the following, which is the main result of this paper.

THEOREM 1. *Let m be an integer greater than or equal to 1. Then*

$$\sum_{r=0}^{m}(-1)^r\binom{m}{r}\binom{m+r}{r}\frac{1}{(r+1)(m+r)} = \begin{cases} 1/2 & \text{if } m=1 \\ 0 & \text{if } m\geq 2. \end{cases} \tag{3}$$

The purpose of this paper is to highlight the various methods of proving combinatorial identities and their applications. We give two proofs of Theorem 1 in Section 2, and discuss alternative methods of proving this and related combinatorial identities. We conclude with a discussion of its application to effective equidistribution in Section 3.

Acknowledgments. We thank Tewodros Amdeberhan, Christian Krattenthaler and the referee for comments on an earlier draft. The first named author would like to thank Cameron and Kayla Miller for quietly sleeping on him while many of the calculations were done. Much of this paper was written when the first two authors attended the Graduate Workshop on L-functions and Random Matrix Theory at Utah Valley University in 2009, and it is a pleasure to thank the organizers.

2. Combinatorial identities

Below we give two different proofs of Theorem 1, each highlighting a different approach to proving combinatorial identities. We first state some needed properties of the binomial coefficients. For n, r non-negative integers we set $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. We generalize to real n and k a positive integer by setting

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-(k-1))}{k!}, \tag{4}$$

which clearly agrees with our original definition for n a positive integer and vanishes when n is a non-negative integer less than k. Finally, we set $\binom{n}{0}=1$ and $\binom{n}{k}=0$ if k is a negative integer.

To prove our main result we need the following two lemmas; we follow the proofs in [20].

LEMMA 1 (Vandermonde's Convolution Lemma). *Let r,s be any two real numbers and k,m,n integers. Then*

$$\sum_k \binom{r}{m+k}\binom{s}{n-k} \;=\; \binom{r+s}{m+n}. \tag{5}$$

Proof. Note that the summand is zero if either $m+k>r$ or $n-k>s$, and thus it is a finite sum over k. It suffices to prove the claim when r,s are integers. The reason is that both sides are polynomials, and if the polynomials agree for an infinitude of integers then they must be identical. By changing n and k, we see it suffices to consider the special case $m=0$, in which case we are reduced to showing

$$\sum_k \binom{r}{k}\binom{s}{n-k} \;=\; \binom{r+s}{n}. \tag{6}$$

Consider the polynomial

$$(x+y)^r(x+y)^s \;=\; (x+y)^{r+s}. \tag{7}$$

If we use the binomial theorem to expand the left hand side of (7), we get the coefficient of the $x^n y^{r+s-n}$ is the left hand side of (6); this follows from looking at all the ways we could get an $x^n y^{r+s-n}$, which involves summing over the coefficients of $x^k y^{r-k}$ times the coefficients of $x^{n-k}y^{s-n+k}$. Similarly, if we use the binomial theorem we find the coefficient of $x^n y^{r+s-n}$ is the right hand side of (7). This proves (6), which completes the proof. □

LEMMA 2. *Let ℓ,m,s be non-negative integers. Then*

$$\sum_k (-1)^k \binom{\ell}{m+k}\binom{s+k}{n} \;=\; (-1)^{\ell+m}\binom{s-m}{n-\ell}. \tag{8}$$

Proof. Using $\binom{a}{b}=\binom{a}{a-b}$, we rewrite $\binom{s+k}{n}$ as $\binom{s+k}{s+k-n}$, and we then rewrite $\binom{s+k}{s+k-n}$ as $(-1)^{s+k-n}\binom{-n-1}{s+k-n}$ by using the extension of the binomial coefficient, where we have pulled out all the negative signs in the numerators. The advantage of this simplification is that the summation index is now only in the denominator; further, the power of -1 is now independent of k. Factoring out the sign, our quantity is equivalent to

$$(-1)^{s-n}\sum_k \binom{\ell}{m+k}\binom{-n-1}{s+k-n} \;=\; (-1)^{s-n}\sum_k \binom{\ell}{\ell-m-k}\binom{-n-1}{s+k-n}, \tag{9}$$

where we again use $\binom{a}{b}=\binom{a}{a-b}$. By Vandermonde's Convolution Lemma, this equals $(-1)^{s-n}\binom{\ell-n-1}{\ell-m-n+s}$. Using $\binom{s-m}{\ell-m-n+s}=\binom{s-m}{n-\ell}$ and collecting powers of -1 completes the proof (note $(-1)^{\ell-m}=(-1)^{\ell+m}$). □

Using the above two lemmas, we can now prove our main result.

First Proof of Theorem 1. The case $m = 1$ follows by direct evaluation. Consider now $m \geq 2$. We have

$$\begin{aligned} S_m &:= \sum_{r=0}^{m} (-1)^r \binom{m}{r}\binom{m+r}{r}\frac{1}{(r+1)(m+r)} \\ &= \sum_{r=0}^{m} (-1)^r \binom{m}{r}\frac{m+1}{m+1}\binom{m+r}{r}\frac{1}{(r+1)(m+r)} \\ &= \sum_{r=0}^{m} (-1)^r \frac{m!(m+1)}{(r+1)\cdot r!m!}\frac{1}{m+1}\ \frac{(m+r)(m+r-1)!}{r!m\cdot(m-1+r)!}\frac{1}{m+r} \qquad (10) \\ &= \sum_{r=0}^{m} (-1)^r \binom{m+1}{r+1}\binom{m-1+r}{r}\frac{1}{m(m+1)} \\ &= \frac{1}{m(m+1)}\sum_{r=0}^{m} (-1)^r \binom{m+1}{r+1}\binom{m-1+r}{m-1}. \end{aligned}$$

We change variables and set $u = r+1$; as r runs from 0 to m, u runs from 1 to $m+1$. To have a complete sum, we want u to start at 0; thus we add in the $u = 0$ term, which is $\binom{m-2}{m-1}$. As $m \geq 2$, this is 0 from the extension of the binomial coefficient (this is the first of two places where we use $m \geq 2$). Our sum S_m thus equals

$$S_m = -\frac{1}{m(m+1)}\sum_{u=0}^{m+1} (-1)^u \binom{m+1}{u}\binom{m-2+u}{m-1}. \qquad (11)$$

We now use Lemma 2 with $k = u$, $m = 0$, $\ell = m+1$, $s = m-2$ and $n = m-1$; note the conditions of that lemma require s to be a non-negative integer, which translates to our $m \geq 2$. We thus find

$$S_m = -\frac{1}{m(m+1)}(-1)^{m+1}\binom{m-2}{-2} = 0, \qquad (12)$$

which completes the proof. □

We give another proof of Theorem 1 below using hypergeometric functions, highlighting other approaches to proving combinatorial identities.

Second Proof of Theorem 1. Consider the hypergeometric function

$${}_2F_1(a,b,c;z) = \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)}\int_0^1 \frac{t^{b-1}(1-t)^{c-b-1}dt}{(1-tz)^a}. \qquad (13)$$

The following identity for the normalization constant of the Beta function is crucial in the expansions:

$$B(x,y) = \int_0^1 t^{x-1}(1-t)^{y-1}dt = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}. \qquad (14)$$

We can use the geometric series formula to expand (13) as a power series in z involving Gamma factors,

$$(15) \qquad {}_2F_1(a,b,c;z) \;=\; \frac{\Gamma(c)}{\Gamma(a)\Gamma(b)} \sum_{n=0}^{\infty} \frac{\Gamma(a+n)\Gamma(b+n)}{\Gamma(c+n)} \frac{z^n}{n!}.$$

Rewriting $\binom{m}{r}$ as $(-1)^r \binom{r-m-1}{r}$, S_m can be written

$$(16) \qquad S_m \;=\; \frac{1}{m!(-m-1)!} \sum_{r=0}^{\infty} \frac{(r-m-1)!(r+m-1)!}{(r+1)!} \frac{1}{r!},$$

where we have formally extended the series to ∞ as the coefficients will vanish for $r \geq m+1$. By comparing the two infinite series and using the fact that $z! = \Gamma(z+1)$, we see that if we take $a = -m$, $b = m$, $c = 2$, $n = r$ and $z = 1$, after some simple algebra we obtain

$$(17) \qquad S_m \;=\; \frac{\Gamma(m)\,{}_2F_1(-m,m,2;1)}{\Gamma(2)\Gamma(1+m)} \;=\; \frac{\Gamma(m)}{\Gamma(1+m)\Gamma(2+m)\Gamma(2-m)},$$

where the last step uses

$$(18) \qquad {}_2F_1(a,b,c;1) \;=\; \frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)},$$

which follows from the normalization constant of the Beta function. Note that the right hand side of (17) equals $1/2$ when $m = 1$ and 0 for $m \geq 2$ because for such m, $1/\Gamma(2-m) = 0$ due to the pole of $\Gamma(2-m)$. □

REMARK 1. It is also possible to prove Theorem 1 through symbolic manipulations. Using the results from [9, 10], one may input this into a Mathematica package, which outputs a proof. The reasoning behind this automated proof method is described in [11], and many of the identities for hypergeometric functions can be interpreted in a very computational manner. These results are also useful in random walk calculations in physics (quantum and classical), and reduction to the hypergeometric function is a convenient first step towards continuum limits or long-time asymptotics.

REMARK 2. We thank the referee for pointing out another approach to proving $S_m = 0$. Let A and B be two vector spaces with $A \cong \mathbb{C}^{m+1}$ and $B \cong \mathbb{C}^m$. Their difference $A - B$ is a virtual vector space whose exterior powers can be evaluated in a consistent fashion as

$$\wedge^m(A-B) \;=\; \bigoplus_{r=0}^{m} (-1)^r \wedge^{m-r} A \otimes S^r B,$$

where $S^r B$ denotes the symmetric product. As $\dim(\wedge^{m-r}A) = \binom{m+1}{r+1}$ and $\dim(S^r B) = \binom{m-1+r}{m-1}$, we obtain the expansion in (10). The proof is completed by noting $A - B$ has virtual dimension 1, so the dimension of its m^{th} exterior power is zero if $m > 1$ and 1 if $m = 1$.

REMARK 3. The combinatorial identity in Theorem 1 is a special case of the Chu–Vandermonde summation formula (see [19]):

$$ {}_2F_1\left(\begin{matrix}a,-n\\ c\end{matrix};1\right) \;=\; \frac{(-a+c)_n}{(c)_n}. \tag{19}$$

We thank Christian Krattenthaler for pointing this out to us.

3. Effective equidistribution

For a sequence of numbers x_n modulo 1, a measure μ and an interval $I \subset [0,1]$, let

$$\begin{aligned} N_I(V_p) &= \#\{n \le V_p : x_n \in I\} \\ \mu(I) &= \int_I \mu(t)dt. \end{aligned} \tag{20}$$

The discrepancy $D_{I,V_p}(\mu)$ is

$$D_{I,V_p}(\mu) \;=\; |N_I(V_p) - V_p\mu(I)|; \tag{21}$$

with this normalization, the goal is to obtain the best possible estimate for how rapidly $D_{I,V_p}(\mu)/V_p$ tends to 0. A standard approach is to use exponential sums and the Erdös–Turan theorem. Modifying the ideas in [7] (see [6] for the details), one finds

THEOREM 2. *Let $\{x_n\} \subset [0,1]$ and let the notation be as above. Let $\{c_m\}$ be a sequence of numbers such that $\sum_{m=-\infty}^{\infty} |c_m| < \infty$. Let $\|\mu\| = \sup_{x\in[0,1]} |F(x)|$ with $\mu = F(-x)dx$. Then for any V_p and M the discrepancy satisfies*

$$D_{I,V_p}(\mu) \le \frac{V_p\|\mu\|}{M+1} + \sum_{1\le m\le M}\left(\frac{1}{M+1} + \min\left(1, \frac{1}{\pi|m|}\right)\right)\left|\sum_{n=1}^{V_p} e(mx_n) - V_pc_m\right|. \tag{22}$$

Let $\mu_{\rm st} = F(-x)dx$ be the normalized Sato–Tate distribution on $[0,1]$. Its density is

$$2\sin^2(\pi x) \;=\; 1 - \tfrac{1}{2}\left(e(x) + e(-x)\right), \quad \text{where} \quad e(x) \;:=\; e^{2\pi i x}, \tag{23}$$

which implies that the coefficients of $\mu_{\rm st}$ are $c_0 = 1$, $c_{\pm 1} = -1/2$ and $c_m = 0$ for $|m| \ge 2$.

We consider the family of all elliptic curves modulo p for $p \ge 5$. We may write these curves in Weierstrass form as $y^2 = x^3 - ax - b$ with $a, b \in \mathbb{Z}/p\mathbb{Z}$ and $4a^3 \ne 27b^2$. The number of pairs (a,b) satisfying these conditions[1] is

$$V_p \;:=\; p(p-1). \tag{24}$$

[1] If $a = 0$ then the only b which is eliminated is $b = 0$. If a is a non-zero perfect square there are two b that fail, while if a is not a square than no b fail. Thus the number of bad pairs of (a,b) is p.

We use Birch's [2] results on the moments of the family of all elliptic curves modulo p (there are some typos in his explicit formulas; we correct these in [6]); unfortunately, these are results for quantities such as $(2\sqrt{p}\cos\theta_n)^{2R}$, and the quantity which naturally arises when applying Theorem 2 is $e(mx_n)$. Here the x_n's are running over the normalized angles $\theta_{a,b}(p)/\pi$. Recall from Section 1 that for an elliptic curve $E: y^2 = x^3 + ax + b$ (with $a, b \in \mathbb{Z}$) we have $a_E(p) = 2\sqrt{p}\cos\theta_{a,b}(p)$, where we may choose $\theta_{a,b}(p) \in [0,\pi]$. We are thus led to study

$$\left|\sum_{n=1}^{V_p} e(mx_n) - V_p c_m\right|. \tag{25}$$

By applying some combinatorial identities we are able to rewrite our sum in terms of the moments, which allows us to use Birch's results. The point of this section is not to obtain the best possible error term but rather to highlight how one may generalize and apply the framework from [7].

We first set some notation. Let $\sigma_k(T_p)$ denote the trace of the Hecke operator T_p acting on the space of cusp forms of dimension $-2k$ on the full modular group. We have $\sigma_{k+1}(T_p) = O(p^{k+c+\varepsilon})$, where from [12] we see we may take $c = 3/4$ (there is no need to use the optimal c, as our final result, namely (41), will yield the same order of magnitude result for $c = 3/4$ or $c = 0$). Let $\mathcal{M}_p(2R)$ denote the $2R^{\text{th}}$ moment of $2\cos(\theta_n) = 2\cos(\pi x_n)$ (as we are concerned with the normalized values, we use slightly different notation than in [2]):

$$\mathcal{M}_p(2R) \;=\; \frac{1}{V_p}\sum_{n=1}^{V_p} (2\cos(\pi x_n))^{2R}. \tag{26}$$

LEMMA 3 (Birch). *With notation as above, we have*

$$\mathcal{M}_p(2R) \;=\; \frac{1}{R+1}\binom{2R}{R} + O\left(2^{2R}V_p^{-\frac{1-c-\varepsilon}{2}}\right); \tag{27}$$

we may take $c = 3/4$ and so there is a power saving (as the exponent of V_p is negative).[2]

Proof. The result follows from dividing the equation for $S_R^*(p)$ on the bottom of page 59 of [2] by p^R, as we are looking at the moments of the normalized Fourier coefficients of the elliptic curves, and then using the bound $\sigma_{k+1}(T_p) = O(p^{k+c+\varepsilon})$, with $c = 3/4$ admissible by [12]. Recall $V_p = p(p-1)$ is the cardinality of the family. We have

$$\begin{aligned}
\mathcal{M}_p(2R) &= \frac{1}{R+1}\binom{2R}{R}\frac{p(p-1)}{V_p} \\
&\quad + O\left(\sum_{k=1}^{R}\frac{2k+1}{R+k+1}\binom{2R}{R+k}\frac{p^{1+c+\varepsilon}}{V_p} + \frac{p}{p^R V_p}\right) \\
&= \frac{1}{R+1}\binom{2R}{R} + O\left(2^{2R}V_p^{-\frac{1-c-\varepsilon}{2}}\right)
\end{aligned} \tag{28}$$

[2] Note $\frac{1}{R+1}\binom{2R}{R}$ is the R^{th} Catalan number. The Catalan numbers are the moments of the semicircle distribution, which is related to the Sato–Tate distribution by a simple change of variables.

since $V_p = p(p-1)$. □

A simple argument[3] shows that the normalized angles are symmetric about $1/2$. This implies

$$\sum_{n=1}^{V_p} e(mx_n) = \sum_{n=1}^{V_p} \cos(2\pi m x_n) + i \sum_{n=1}^{V_p} \sin(2\pi m x_n) = \sum_{n=1}^{V_p} \cos(2m\theta_n), \tag{29}$$

where the sine piece does not contribute as the angles are symmetric about $1/2$. Thus it suffices to show we have a power saving in

$$\left| \sum_{n=1}^{V_p} \cos(2m\theta_n) - V_p c_m \right|. \tag{30}$$

By symmetry, it suffices to consider $m \geq 0$.

LEMMA 4. *Let $c_0 = 1$, $c_{\pm 1} = -1/2$ and $c_m = 0$ otherwise. There is some $c < 1$ such that*

$$\left| \sum_{n=1}^{V_p} \cos(2m\theta_n) - V_p c_m \right| \ll \left(m^2 2^{3m} V_p^{-\frac{1-c-\varepsilon}{2}} \right); \tag{31}$$

by the work of Selberg [12] we may take $c = 3/4$.

Proof. The case $m = 0$ is trivial. For $m = 1$ we use the trigonometric identity $\cos(2\theta_n) = 2\cos^2(\theta_n) - 1$. As $c_{\pm 1} = -1/2$ we have

$$\begin{aligned} \sum_{n=1}^{V_p} \cos(2\theta_n) - \frac{V_p}{2} &= \sum_{n=1}^{V_p} \left[\left(2\cos^2\theta_n - 1\right) + \frac{1}{2} \right] \\ &= \frac{1}{2} \sum_{n=1}^{V_p} \left((2\cos\theta_n)^2 - 1 \right) \\ &= \frac{1}{2} \sum_{n=1}^{V_p} \left(\frac{(2\sqrt{p}\cos\theta_n)^2}{p} - 1 \right). \end{aligned} \tag{32}$$

Note the sum of $(2\sqrt{p}\cos\theta_n)^2$ is the second moment of the number of solutions modulo p. From [2] we have that this is $p + O(1)$; the explicit formula given in [2] for the second moment is wrong; see [6] for the correct statement. Substituting yields

$$\left| \sum_{n=1}^{V_p} \cos(2\theta_n) - \frac{V_p}{2} \right| \ll O(1). \tag{33}$$

[3] To see that we may match the angles as claimed for the family of all elliptic curves, consider the elliptic curve $y^2 = x^3 - ax - b$ with $4a^3 \neq 27b^2$. Let c be any non-residue modulo p, and consider the curve $y^2 = x^3 - ac^2x - bc^3$. Using the Legendre sum expressions for $a_E(p)$ and $a_{E'}(p)$, using the automorphism $x \to cx$ we see the second equals $\left(\frac{c}{p}\right)$ times the first; as we have chosen c to be a non-residue, this means $2\sqrt{p}\cos(\theta_{E'}(p)) = -2\sqrt{p}\cos(\theta_E(p))$, or $\theta_{E'}(p) = \pi - \theta_E(p)$ as claimed.

The proof is completed by showing that $\sum_{n=1}^{V_p}\cos(2m\theta_n) = O_m(V_p^{1/2})$ provided $2 \le m \le M$. In order to obtain the best possible results, it is important to understand the implied constants, as M will have to grow with V_p (which is of size p^2). While it is possible to analyze this sum for any m by brute force, we must have M growing with p, and so we need an argument that works in general. As $c_{\pm 1} \neq 0$ but $c_m = 0$ for $|m| \ge 2$, we expect (and will see) that the argument below does break down when $|m| = 1$.

There are many possible combinatorial identities we can use in order to express $\cos(2m\theta_n)$ in terms of powers of $\cos(\theta_n)$. We choose the following (for a proof, see Definition 2 and equation (3.1) of [5]):

$$2\cos(2m\theta_n) \;=\; \sum_{r=0}^{m} c_{2m,2r}(2\cos\theta_n)^{2r}, \tag{34}$$

where $c_{2r} = (2r)!/2$, $c_{0,0} = 0$, $c_{2m,0} = (-1)^m 2$ for $m \ge 1$, and for $1 \le r \le m$ set

$$c_{2m,2r} \;=\; \frac{(-1)^{r+m}}{c_{2r}}\prod_{j=0}^{r-1}(m^2-j^2) \;=\; \frac{(-1)^{m+r}}{c_{2r}}\frac{m\cdot(m+r-1)!}{(m-r)!}. \tag{35}$$

We now sum (34) over n and divide by V_p, the cardinality of the family. In the argument below, at one point we replace 2^{2r} in an error term with $2012\frac{1}{r+1}\binom{2r}{r}\cdot m^2$; this allows us to pull the r^{th} Catalan number, $\frac{1}{r+1}\binom{2r}{r}$, out of the error term.[4] Using Lemma 3 we find that

$$\begin{aligned}
\frac{1}{V_p}\sum_{n=1}^{V_p} 2\cos(2m\theta_n) \;&=\; \sum_{r=0}^{m} c_{2m,2r}\frac{1}{V_p}\sum_{n=1}^{V_p}(2\cos\theta_n)^{2r} \\
&= \sum_{r=0}^{m}\left(\frac{1}{r+1}\binom{2r}{r} + O\left(2^{2r}V_p^{-\frac{1-c-\varepsilon}{2}}\right)\right)c_{2m,2r} \\
&= \sum_{r=0}^{m}\left(\frac{1}{r+1}\frac{(2r)!}{r!r!}\frac{(-1)^{m+r}2}{(2r)!}\frac{m\cdot(m+r)!}{(m-r)!\cdot(m+r)}\right) \\
&\qquad\cdot\left(1+O\left(m^2V_p^{-\frac{1-c-\varepsilon}{2}}\right)\right) \qquad (36)\\
&= (-1)^m 2m\sum_{r=0}^{m}\left((-1)^r\frac{m!}{r!(m-r)!}\frac{(m+r)!}{m!r!}\frac{1}{(r+1)(m+r)}\right) \\
&\qquad\cdot\left(1+O\left(m^2V_p^{-\frac{1-c-\varepsilon}{2}}\right)\right) \\
&= (-1)^m 2m\sum_{r=0}^{m}\left((-1)^r\binom{m}{r}\binom{m+r}{r}\frac{1}{(r+1)(m+r)}\right) \\
&\qquad\cdot\left(1+O\left(m^2V_p^{-\frac{1-c-\varepsilon}{2}}\right)\right).
\end{aligned}$$

[4] The reason this is valid is that the largest binomial coefficient is the middle (or the middle two when the upper argument is odd). Thus $2^{2r} = (1+1)^{2r} \le (2r+1)\binom{2r}{r} \le 2(m+1)\binom{2r}{r}$ (as $m \le r$), and the claim follows from $\frac{2012m^2}{r+1} \ge 2(m+1)$ for $m \ge 2$ and $0 \le r \le m$.

We first bound the error term. For our range of r, $\binom{m+r}{r} \le \binom{2m}{m} \le 2^{2m}$. The sum of $\binom{m}{r}$ over r is 2^m, and we get to divide by at least $m+r \ge m$. Thus the error term is bounded by

$$O\left(m^2 2^{3m} V_p^{-\frac{1-c-\varepsilon}{2}}\right).$$

We now turn to the main term. It it just $(-1)^m 2m$ times the sum in Theorem 1, which is shown in that theorem to equal 0 for any $|m| \ge 2$. Note that without Theorem 1, our combinatorial expansion would be useless. □

REMARK 4. It is possible to get a better estimate for the error term by a more detailed analysis of $\sum_{r\le m}\binom{m}{r}\binom{m+r}{r}$; however, the improved estimates only change the constants in the discrepancy estimates, and not the savings. This is because this sum is at least as large as the term when $r \approx m/2$, and this term contributes something of the order $3^{3m/2}/m$ by Stirling's formula. We will see that any error term of size 3^{am} for a fixed a gives roughly the same value for the best cutoff choice for M, differing only by constants. Thus we do not bother giving a more detailed analysis to optimize the error here.

We now prove effective equidistribution for the family of all elliptic curves.

THEOREM 3. *For the family of all elliptic curves modulo p, as $p \to \infty$ we have*

$$D_{I,V_p}(\mu_{\mathrm{st}}) \;\le\; C\frac{V_p}{\log V_p} \tag{37}$$

for some computable C.

Proof. We must determine the optimal M to use in (22):

$$\begin{aligned} D_{I,V_p}(\mu_{\mathrm{st}}) &\ll \frac{V_p}{M+1} + \sum_{1\le m\le M}\left(\frac{1}{M+1}+\frac{1}{m}\right)\left(m^2 2^{3m} V_p^{-\frac{1-c-\varepsilon}{2}}\right) \\ &\ll \frac{V_p}{M} + M 2^{3M} V_p^{-\frac{1-c-\varepsilon}{2}} \qquad (38) \end{aligned}$$

as $\frac{1}{M+1} \ll \frac{1}{m}$ and $\sum_{m\le m} 2^{3m} \ll 2^{3M}$. For all $c > 0$ we find the minimum error by setting the two terms equal to each other, which yields

$$V_p^{\frac{3-c-\varepsilon}{2}} \;=\; M^2 2^{3M}. \tag{39}$$

For ease of exposition we replace $M^2 2^{3M}$ with e^{3M}; this worsens our constant slightly, but does not qualitatively change the result. Equating these errors means we are looking for M such that

$$e^{3M} \;=\; e^{\frac{3-c-\varepsilon}{2}\log V_p}, \tag{40}$$

which implies

$$M \;=\; \frac{3-c-\varepsilon}{6}\log V_p. \tag{41}$$

We thus see that we may find a constant C such that

$$D_{I,V_p}(\mu_{\mathrm{st}}) \leq C\frac{V_p}{\log V_p}. \tag{42}$$

This yields a logarithm savings in the discrepancy, and proves effective equidistribution. □

References

[1] BANKS W. D. AND SHPARLINSKI I. E. Sato-tate, cyclicity, and divisibility statistics on average for elliptic curves of small height. *Israel J. Math. 173* (2009), 253–277.

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

[3] KATZ N. *Gauss Sums, Kloosterman Sums, and Monodromy Groups*. Princeton University Press, Princeton, NJ, 1988.

[4] MICHEL P. Rang moyen de familles de courbes elliptiques et lois de Sato-Tate. *Monat. Math. 120* (1995), 127–136.

[5] MILLER S. J. An identity for sums of polylogarithm functions. *Integers: Electronic Journal Of Combinatorial Number Theory 8* (2008), #A15.

[6] MILLER S. J. AND MURTY M. R. Effective equidistribution and the Sato-Tate law for families of elliptic curves. *J. Number Theory 131*, 1 (2011), 25–44.

[7] MURTY M. R. AND SINHA K. Effective equidistribution of eigenvalues of Hecke operators. *J. Number Theory 129*, 3 (2009), 681–714.

[8] NIEDERREITER H. The distribution of values of Kloosterman sums. *Arch. Math. 56* (1991), 270–277.

[9] PAULE P. AND SCHORN M. A mathematica version of Zeilberger's algorithm for proving binomial coefficient identities. *J. Symbolic Computation 11* (1994), 1–25.

[10] PAULE P., SCHORN M. AND RIESE A. An implementation of Zeilberger's fast algorithm. `http://www.risc.uni-linz.ac.at/research/combinat/software/PauleSchorn/index.php`.

[11] PETKOVSEK M., WILF H. AND ZEILBERGER D. $A = B$. A. K. Peters, 1996, `http://www.math.upenn.edu/~wilf/AeqB.html`.

[12] SELBERG A. On the estimation of Fourier coefficients of modular forms. In *Theory of Numbers (Pasedena, 1963)*, Proc. Sympos. Pure Math., Vol. VIII. Amer. Math. Soc., Providence, 1965, pp. 1–15.

[13] SERRE J.-P. Répartition asymptotique des valuers propres de l'opérateur de Hecke T_p. *J. Amer. Math. Soc. 10*, 1 (1997), 75–102.

[14] SHPARLINSKI I. E. On the Lang-Trotter and Sato-Tate conjectures on average for some families of elliptic curves. Preprint.

[15] SHPARLINSKI I. E. On the Sato-Tate conjecture on average for some families of elliptic curves. Preprint.

[16] SILVERMAN J. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics 106. Springer-Verlag, New York-Berlin, 1986.

[17] SILVERMAN J. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics 151. Springer-Verlag, New York-Berlin, 1994.

[18] SILVERMAN J. AND TATE J. *Rational Points on Elliptic Curves*. Springer-Verlag, New York, 1992.

[19] SLATER L. *Generalized Hypergeometric Functions*. Cambridge University Press, 2008.

[20] WARD K. J. Series sums of binomial coefficients. http://www.trans4mind.com/personal_development/mathematics/series/summingBinomialCoefficients.htm.

AMS Subject Classification: 05A40, 05A10; 33C05, 11K38, 14H52, 11M41

Steven J. MILLER
Department of Mathematics and Statistics, Williams College
Williamstown, MA 01267, USA
e-mail: Steven.J.Miller@williams.edu

M. RAM MURTY
Department of Mathematics, Queen's University
Kingston, Ontario, K7L 3N6, CANADA
e-mail: murty@mast.queensu.ca

Frederick STRAUCH
Department of Physics, Williams College
Williamstown, MA 01267, USA
e-mail: fws1@williams.edu

Lavoro pervenuto in redazione il 01.08.2010 e, in forma definitiva, il 28.09.2010