EQUIDISTRIBUTION OF HECKE POINTS ON THE SUPERSINGULAR MODULE

RICARDO MENARES

Abstract. For a fixed prime p, we consider the (finite) set of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Hecke operators act on this set. We compute the asymptotic frequence with which a given supersingular elliptic curve visits another under this action.

1. Introduction

Let p be a prime number. We denote by $E = \{E_1, \dots, E_n\}$ the set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. We denote by $S := \oplus_{i=1}^n \mathbb{Z}E_i$ the supersingular module in characteristic p (i.e. S is the free abelian group spanned by the elements of E). Hecke operators act on S by

$$T_1 := id, \quad T_m(E_i) = \sum_C E_i/C, \quad m \geq 2,$$

where C runs through the subgroup schemes of E_i of rank m. This definition is extended by linearity to S and to $S_{\mathbb{R}} := S \otimes \mathbb{R}$. For an integer $m \geq 1$ we put

$$B_{i,j}(m) = |\{C \subset E_i, \quad |C| = m \text{ et } E_i/C \cong E_j\}|.$$

We have that $T_m E_i = \sum_{j=1}^n B_{i,j}(m) E_j$. The the matrix $\big(B_{i,j}(m)\big)_{i,j=1}^n$ is known as the Brandt matrix of order m.

For a given $D = \sum_{i=1}^n a_i E_i \in S_{\mathbb{R}}$, we put $\deg D = \sum_{i=1}^n a_i$. We have that ([4], Propositon 2.7)

$$\deg T_m E_i = \sum_{\substack{d|m \\ p\nmid d}} d =: \sigma_p(m),$$

leading to define $\deg T_m := \sigma_p(m)$.

Let M be the set of probability measures on E. For every $i = 1, \dots, n$, we denote by $\delta_{E_i} \in M$ the Dirac measure supported on E_i. Let

$$S^+ := \Big\{ \sum_{i=1}^n a_i E_i \in S_{\mathbb{R}} \text{ such that } a_i \geq 0 \Big\} - \{0\}.$$

For any $D = \sum_{i=1}^n a_i E_i \in S^+$, we put

$$\Theta_D := \frac{1}{\deg D} \sum_{i=1}^n a_i \delta_{E_i}.$$

We have that Θ_D is a probability measure on E and every element of M has this form. Hence, there is a natural action of the Hecke operators on M, given by $T_m \Theta_D := \Theta_{T_m D}$.

Each E_i has a finite number of automorphisms. We define

$$w_i := |\mathrm{Aut}(E_i)/\{\pm 1\}|, \quad W := \sum_{i=1}^n \frac{1}{w_i}.$$

The element $e := \sum_{i=1}^{n} \frac{1}{w_i} E_i \in S \otimes \mathbb{Q}$ is Eisenstein ([4], p. 139), i.e.

$$T_m(e) = \deg T_m e. \tag{1.1}$$

We denote by $\Theta := \Theta_e$. Equation (1.1) implies that $T_m \Theta = \Theta$ for all $m \geq 1$.

Let $C(E) \cong \mathbb{C}^n$ be the space of complex valued functions on E. For $f \in C(E)$, we denote by $\|f\| = \max_i |f(E_i)|$ and $\Theta_D(f) = (\deg D)^{-1} \sum a_i f(E_i)$. For a positive integer m, we write $m = p^k m_p$ with $p \nmid m_p$. We obtain the following result:

Theorem 1.1. *For all $i = 1, \ldots, n$, the sequence of measures $\{\Theta_{T_m E_i}\}$, where m runs through a set of positive integers such that m_p is unbounded, is equidistributed with respect to Θ. More precisely, for all $\varepsilon > 0$, there exists $C_\varepsilon > 0$ such that for every sequence of integers m such that $m_p \to \infty$, we have that*

$$|\Theta_{T_m E_i}(f) - \Theta(f)| \leq C_\varepsilon \|f\| n m^{-\frac{1}{2}+\varepsilon}.$$

We study the asymtotic frequence of the multiplicity of E_j inside $T_m E_i$. That is, the behavoir of the ratio $B_{i,j}(m)/\deg(T_m)$ when m varies. We will prove Theorem 1.1 in the equivalent formulation:

Theorem 1.2. *For all $\varepsilon > 0$, there exists $C_\varepsilon > 0$ such that for every sequence of integers m such that $m_p \to \infty$, we have that*

$$\Big| \frac{B_{i,j}(m)}{\deg T_m} - \frac{12}{w_j(p-1)} \Big| \leq C_\varepsilon m^{-\frac{1}{2}+\varepsilon}. \tag{1.2}$$

In particular,

$$\lim_{m_p \to \infty} \frac{B_{i,j}(m)}{\deg T_m} = \frac{12}{w_j(p-1)}. \tag{1.3}$$

The proof of this assertion is found in section 1.2.

Remark 1.3. The equality $\sum_{j=1}^{n} \frac{B_{i,j}(m)}{\deg T_m} = 1$, combined with equation (1.3) implies the mass formula of Deuring and Eichler:

$$W = \sum_{j=1}^{n} \frac{1}{w_j} = \frac{p-1}{12}.$$

Theorem 1.1 can be deduced from Theorem 1.2 as follows: remark 1.3 implies that $\Theta = \sum_{j=1}^{n} \frac{12}{w_j(p-1)} \delta_{E_j}$. Take $f \in C^0(E)$. We have that

$$|\Theta_{T_m E_i}(f) - \Theta(f)| \leq \|f\| \sum_{j=1}^{n} \Big| \frac{B_{i,j}(m)}{\deg T_m} - \frac{12}{w_j(p-1)} \Big|.$$

Hence, inequality (1.2) implies Theorem 1.1.

Let $h : E \to E$ be a function. Then h defines an endomorphism of S and of $S_{\mathbb{R}}$ by the rule

$$h\Big(\sum a_i E_i\Big) := \sum a_i h(E_i).$$

We will also consider the action induced on M by $h^* \Theta_D := \Theta_{h(D)}$.

Corollary 1.4. *Let $q \neq p$ be a prime number. Let $h : E \to E$ be a function such that $h \circ T_q = T_q \circ h$. Then $h^* \Theta = \Theta$. In other words, h can be identified with a permutation $\tau \in S_n$ by $h(E_i) = E_{\tau(i)}$ and we have that $w_i = w_{\tau(i)}$ for all $i = 1, \ldots, n$.*

Proof: since T_{q^k} is a polynomial in T_q, we also have that $h \circ T_{q^k} = T_{q^k} \circ h$. Let $f \in C(E)$. We have that

$$\begin{aligned}
h^*\Theta(f) &= \lim_{k\to\infty} h^*\Theta_{T_{q^k}E_1}(f) && (1.4)\\
&= \lim_{k\to\infty} \Theta_{h\circ T_{q^k}E_1}(f)\\
&= \lim_{k\to\infty} \Theta_{T_{q^k}\left(h(E_1)\right)}(f)\\
&= \Theta(f), && (1.5)
\end{aligned}$$

where we have used Theorem 1.1 in (1.4) and (1.5) ■

The statement Theorem 1.1, using the Hecke invariant measure Θ, has been included to emphasize the analogy with the fact that Hecke orbits are equidistributed on the modular curve $SL_2(\mathbb{Z})\backslash\mathbb{H}$ with respect to the hyperbolic measure, which is Hecke invariant (e.g. see [1], Section 2).

1.1. **Weight 2 Eisenstein series for $\Gamma_0(p)$.** The modular curve $X_0(p)$ has two cusps, represented by 0 and ∞. We denote by Γ_∞ (resp. Γ_0) the stabilizer of ∞ (resp. 0). The associated weight 2 Eisenstein series are given by

$$\begin{aligned}
E_\infty(z) &= \frac{1}{2}\lim_{\varepsilon\to0^+}\sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(p)} j_\gamma(z)^{-2}|j_\gamma(z)|^{-2\varepsilon}\\
E_0(z) &= \frac{1}{2}\lim_{\varepsilon\to0^+}\sum_{\gamma\in\Gamma_0\backslash\Gamma_0(p)} j_{\sigma_0^{-1}\gamma}(z)^{-2}|j_{\sigma_0^{-1}\gamma}(z)|^{-2\varepsilon},
\end{aligned}$$

where $\sigma_0 = \begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & 0 \end{pmatrix}$ and $j_\eta(z) = cz + f$ for $\eta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

The functions E_∞ and E_0 are weight 2 modular forms for $\Gamma_0(p)$ and they are Hecke eigenforms. The Fourier expansions at $i\infty$ are ([5], Theorem 7.2.12, p. 288)

$$\begin{aligned}
E_\infty(z) &= 1 - \frac{3}{\pi y(p+1)} + \frac{24}{p^2-1}\sum_{n=1}^{\infty} b_n q^n\\
E_0(z) &= -\frac{3}{\pi y(p+1)} - \frac{24p}{p^2-1}\sum_{n=1}^{\infty} a_n q^n,
\end{aligned}$$

with the sequences a_n and b_n given by:

- if $p \nmid n$, then $a_n = b_n = \sigma_1(n)$
- if $k \geq 1$, then $b_{p^k} = p + 1 - p^{k+1}$ and $a_{p^k} = p^k$
- if $p \nmid m$ and $k \geq 1$, then $b_{p^k m} = -b_{p^k} b_m$ and $a_{p^k m} = a_{p^k} a_m$.

By taking an appropriate linear combination, we obtain a non cuspidal, holomorphic at $i\infty$ modular form

$$\begin{aligned}
f_0(z) &:= E_\infty(z) - E_0(z)\\
&= 1 + \frac{24}{p^2-1}\sum_{n=1}^{\infty}(pa_n + b_n)q^n.
\end{aligned}$$

Since we have that

$$\begin{aligned} E_\infty|_{\sigma_0}(z) &= E_0(z) \\ E_0|_{\sigma_0}(z) &= E_\infty(z), \end{aligned}$$

this shows that f is holomorphic at $\Gamma_0(p)0$ aswell. Since

$$\dim_{\mathbb{C}} M_2(\Gamma_0(p)) = 1 + \dim_{\mathbb{C}} S_2\big(\Gamma_0(p)\big)$$

and since f is holomorphic, non zero and non cuspidal, we have the decomposition

$$M_2(\Gamma_0(p)) = S_2(\Gamma_0(p)) \oplus \mathbb{C} f_0. \tag{1.6}$$

1.2. **Proof of Theorem 1.2.** Recall that we write $m = p^k m_p$ with $p \nmid m_p$. We have that $B(p^k)$ is a permutation matrix of order dividing 2 and that $B(m) = B(p^k)B(m_p)$ ([4], Proposition 2.7). It follows that $\deg(T_m) = \deg(T_{m_p})$ and that we can define, for each $i = 1, \ldots, n$, an index $i(k) \in \{1, \ldots, n\}$ such that $B_{i,l}(p^k) = \delta_{i(k),l}$. Furthermore, $i(k) = i$ if k is even. We have that

$$\begin{aligned} \frac{B_{i,j}(m)}{\deg T_m} &= \sum_{l=1}^{n} \frac{B_{i,l}(p^k) B_{l,j}(m_p)}{\deg T_{m_p}} \\ &= \frac{B_{i(k),j}(m_p)}{\deg T_{m_p}}. \end{aligned}$$

Hence, to prove Theorem 1.2 we may assume $p \nmid m$, which is what we will do in what follows.

Our method is based on the interpretation of the multiplicities $B_{i,j}(m)$ as Fourier coefficients of a modular form.

Theorem 1.5. *([4], Proposition 2.3 and [3], Chapter II, Theorem 1) For every* $0 \leq i, j \leq n$, *there exists a weight 2 modular form* $f_{i,j}$ *for* $\Gamma_0(p)$ *such that its* q*-expansion at* ∞ *is*

$$f_{i,j}(z) := \frac{1}{2w_j} + \sum_{m=1}^{\infty} B_{i,j}(m) q^m, \quad q = e^{2\pi i z}.$$

Using (1.6), we can decompose

$$f_{i,j} = g + c f_0, \quad g \in S_2(\Gamma_0(p)), \quad c \in \mathbb{C}.$$

Comparing the q-expansions, we get $c = \frac{1}{2w_j}$. We have that

$$g = f_{i,j} - c f_0 = \sum_{m=1}^{\infty} c_m q^m,$$

where

$$c_m = B_{i,j}(m) - \frac{12}{w_j(p^2-1)}(p a_m + b_m).$$

Since $p \nmid m$, we have that $\deg(T_m) = \sigma_1(m)$ and

$$c_m = B_{i,j}(m) - \frac{12}{w_j(p-1)} \sigma_1(m).$$

Hence,

$$\begin{aligned}\Big|\frac{B_{i,j}(m)}{\deg T_m} - \frac{12}{w_j(p-1)}\Big| &= \frac{|c_m|}{\sigma_1(m)} \\ &\leq \frac{|c_m|}{m}.\end{aligned}$$

Using Deligne's theorem ([2], théorème 8.2, previously Ramanujan's conjecture), we have that

$$c_m = O_\varepsilon(m^{1/2+\varepsilon}),$$

concluding the proof. ■

References

[1] Laurent Clozel and Emmanuel Ullmo. Équidistribution des points de Hecke. In *Contributions to automorphic forms, geometry, and number theory*, pages 193–254. Johns Hopkins Univ. Press, Baltimore, MD, 2004.

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

[3] M. Eichler. The basis problem for modular forms and the traces of the Hecke operators. In *Modular functions of one variable, I (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 75–151. Lecture Notes in Math., Vol. 320. Springer, Berlin, 1973.

[4] Benedict H. Gross. Heights and the special values of L-series. In *Number theory (Montreal, Que., 1985)*, volume 7 of *CMS Conf. Proc.*, pages 115–187. Amer. Math. Soc., Providence, RI, 1987.

[5] Toshitsune Miyake. *Modular forms.* Springer-Verlag, Berlin, 1989. Translated from the Japanese by Yoshitaka Maeda.

Facultad de Matemáticas, PUC, Vicuña Mackenna 4860, Santiago, Chile

E-mail address: rmenares@mat.puc.cl