Diophantine m-tuples in finite fields and modular forms

Andrej Dujella and Matija Kazalicki

Abstract

For a prime p, a Diophantine m-tuple in $\mathbb{F}_p$ is a set of m nonzero elements of $\mathbb{F}_p$ with the property that the product of any two of its distinct elements is one less than a square.

In this paper, we present formulas for the number $N^{(m)}(p)$ of Diophantine m-tuples in $\mathbb{F}_p$ for $m = 2, 3$ and 4. Fourier coefficients of certain modular forms appear in the formula for the number of Diophantine quadruples.

We prove that asymptotically $N^{(m)}(p) = \frac{1}{2^{\binom{m}{2}}}\frac{p^m}{m!} + o(p^m)$, and also show that if $p > 2^{2m-2}m^2$, then there is at least one Diophantine m-tuple in $\mathbb{F}_p$.

1. Introduction

A Diophantine m-tuple is a set of m positive integers with the property that the product of any two of its distinct elements is one less than a square. If a set of nonzero rationals has the same property, then it is called a rational Diophantine m-tuple. Diophantus of Alexandria found the first example of a rational Diophantine quadruple $\{1/16, 33/16, 17/4, 105/16\}$, while the first Diophantine quadruple in integers was found by Fermat, and it was the set $\{1, 3, 8, 120\}$. It was proved in [Duj04] that an integer Diophantine sextuple does not exist and that there are only finitely many such quintuples. Recently, He, Togbé and Ziegler [HTZ] proved there does not exist an integer Diophantine quintuple. On the other hand, it was shown in [DKMS16] that there are infinitely many rational Diophantine sextuples (for another construction see [DujKaz]), and it is not known if there are rational Diophantine septuples. For a short survey on Diophantine m-tuples see [Duj16].

One can study Diophantine m-tuples over any commutative ring with unity. In this paper, we consider Diophantine m-tuples in finite fields $\mathbb{F}_p$, where p is an odd prime. In this setting, it is natural to ask about the number $N^{(m)}(p)$ of Diophantine m-tuples with elements in $\mathbb{F}_p$ (we consider 0 to be a square in $\mathbb{F}_p$).

Since half of the elements of $\mathbb{F}_p^\times$ are squares, heuristically, one expects that a randomly chosen m-tuple of different elements in $\mathbb{F}_p^\times$ will have the Diophantine property with probability $\frac{1}{2^{\binom{m}{2}}}$, i.e. we expect $N^{(m)}(p) = \frac{1}{2^{\binom{m}{2}}}\frac{p^m}{m!} + o(p^m)$. We prove this asymptotic formula at the end of Section 6.

We can describe numbers $N^{(m)}(p)$ geometrically in the following way. Let V_m be the m

2010 Mathematics Subject Classification 11G25, 11F80 (primary), 11T24 (secondary)
Keywords: Diophantine m-tuples, modular forms, finite fields, elliptic curves

dimensional variety in $m+\binom{m}{2}$ dimensional affine space given by the equations $a_ia_j+1=t_{ij}^2$ for $1\leqslant i<j\leqslant m$, where the coordinates are a_i for $1\leqslant i\leqslant m$ and t_{ij} for $1\leqslant i<j\leqslant m$. Let $U_m\subset V_m$ be the open subset where all a_i are nonzero and pairwise distinct. The group $G_m=\{\pm 1\}^{\binom{m}{2}}\rtimes S_m$ acts on V_m and on U_m, the first factor by changing the signs of t_{ij} and the second by permuting the indices. Then $N^{(m)}(p)$ is the number of G_m-orbits in $U_m(\mathbb{F}_p)$.

The main theorem of the paper gives an exact formula for the number of Diophantine quadruples $N^{(4)}(p)$ given in terms of the Fourier coefficients of the following modular forms.

Let

$$f_1(\tau)=\sum_{n=1}^{\infty}b(n)q^n\in S_3\left(\Gamma_0(8),\left(\frac{-2}{\bullet}\right)\right),$$
$$f_2(\tau)=\sum_{n=1}^{\infty}c(n)q^n\in S_3\left(\Gamma_0(16),\left(\frac{-4}{\bullet}\right)\right),$$
$$f_3(\tau)=\sum_{n=1}^{\infty}d(n)q^n\in S_4\left(\Gamma_0(8)\right),$$
$$f_4(\tau)=\sum_{n=1}^{\infty}e(n)q^n\in S_5\left(\Gamma_0(4),\left(\frac{-4}{\bullet}\right)\right),$$

be the unique rational newforms in the corresponding spaces of modular forms. Here $S_k(\Gamma_0(N),\chi)$ denotes the space of cusp forms of weight k, level N and nebentypus χ. Note that all modular forms except $f_3(\tau)$ are CM forms so we have explicit formulas for their Fourier coefficients which are given in Section 4.2.

Theorem 1. *Let p be an odd prime. Denote by $q(p)=e(p)-6d(p)+24b(p)-24c(p)$. Then, the number $N^{(4)}(p)$ of Diophantine quadruples over $\mathbb{F}_p$ is given by the following formula:*

$$N^{(4)}(p)=\begin{cases}\frac{1}{24\cdot 64}\left(p^4-24p^3+206p^2-650p+477+q(p)\right), & \text{if } p\equiv 1 \pmod 8,\\ \frac{1}{24\cdot 64}\left(p^4-24p^3+236p^2-1098p+1761+q(p)\right), & \text{if } p\equiv 3 \pmod 8,\\ \frac{1}{24\cdot 64}\left(p^4-24p^3+206p^2-698p+573+q(p)\right), & \text{if } p\equiv 5 \pmod 8,\\ \frac{1}{24\cdot 64}\left(p^4-24p^3+236p^2-1050p+1761+q(p)\right), & \text{if } p\equiv 7 \pmod 8.\end{cases}$$

An elementary upper bound for the Fourier coefficients of cusp forms (see Chapter 5 of [Iwa97]) implies that $q(p)=O(p^{5/2})$, so we have $N^{(4)}(p)=\frac{1}{24\cdot 64}p^4+O(p^3)$, which is consistent with the heuristics mentioned earlier.

In addition to this, using a more elementary approach of character sums, in Proposition 18 we derive formulas for the number of Diophantine pairs $N^{(2)}(p)$, and in Proposition 21, by mapping V_3 birationally to the affine hypersurface given by $(x^2-1)(y^2-1)=z^2-w^2$, we derive formula for the number of Diophantine triples $N^{(3)}(p)$ in $\mathbb{F}_p$.

For a general m it is natural to ask how large p must be so that there is at least one Diophantine m-tuple in $\mathbb{F}_p$. In Theorem 17, we prove that this is the case if $p>2^{2m-2}m^2$.

The rest of the paper is organized as follows. In Section 2, we construct a 2-to-1 map $V_4\to\mathcal{C}$, where $\mathcal{C}$ is fiber cube of the curve $\mathcal{D}_t:(x^2-1)(y^2-1)=t$ over $\mathbb{P}^1$. This map give rise to a correspondence between the set of Diophantine quadruples $\{a,b,c,d\}$ and the set of admissible triples (Q_1,Q_2,Q_3) of $\mathbb{F}_p$-points on the curve $\mathcal{D}_t$, for some $t\in\mathbb{F}_p^{\times}$ such that each admissible triple corresponds to one or two Diophantine quadruples. If $t\neq 0,1$, the curve $\mathcal{D}_t$ is birationally

equivalent to the elliptic curve $E_t : V^2 = U^3 - 2(t-2)U^2 + t^2U$, with the distinguished point $R = (t, 2t)$ of order 4. Hence we identify $\mathcal{D}_t(\mathbb{F}_p)$ with $\tilde{E}_t(\mathbb{F}_p) := E_t(\mathbb{F}_p) \setminus \{\mathcal{O}, R, 2R, 3R\}$.

If $t \neq 0, 1$ we say that the triple (Q_1, Q_2, Q_3) of points on $\tilde{E}_t(\mathbb{F}_p)$ is admissible if and only if $U(Q_1 + Q_2 + Q_3 + R)$ is a square, and if for no two Q_i and Q_j with $i \neq j$, we have that $Q_i = \pm Q_j + kR$, where $k \in \{0, 1, 2, 3\}$. For the definition of admissibility when $t = 1$ see the end of Section 2.

In Section 3, we find a formula for $N^{(4)}(p)$ by counting admissible triples on $\tilde{E}_t(\mathbb{F}_p)$ for each t. The formula can be written as a linear combination of sums of the form $\sum_{t \in X(\mathbb{F}_p)} P(t)^k$, where X is one of the modular curves (for definitions see Section 4.1)

$$X_1(4), X_1(8), X(2,4), X(2,8)$$

and $P(t)$ is the number of $\mathbb{F}_p$-rational points on the fiber above t of the universal elliptic curve over the modular curve X, and $k \in \{0, 1, 2, 3\}$.

In Section 4, using universal elliptic curves over the modular curves introduced above, we define certain compatible families of ℓ-adic Galois representations such that the trace of Frobenius $Frob_p$ under these representations is essentially equal to the sums above. On the other hand, these representations are isomorphic to the ℓ-adic realizations of the motives associated to the spaces of cusps forms of weight $k+2$ on the corresponding groups, which enables us to express the traces of Frobenius in terms of the coefficients of the Hecke eigenforms in those spaces.

In Section 5, using the methods from the previous section we calculate in Propositions 13-16 the sums from the formula for $N^{(4)}(p)$, and prove Theorem 1.

In Section 6 we obtain formulas for $N^{(2)}(p)$ and $N^{(3)}(p)$, and prove Theorem 17 together with an asymptotic formula for $N^{(m)}(p)$.

2. Correspondence

Let (a, b, c, d) be ordered Diophantine quadruple with elements in $\mathbb{F}_p$, and let

$$ab + 1 = t_{12}^2, \quad ac + 1 = t_{13}^2, \quad ad + 1 = t_{14}^2,$$
$$bc + 1 = t_{23}^2, \quad bd + 1 = t_{24}^2, \quad cd + 1 = t_{34}^2.$$

It follows that $(t_{12}, t_{34}, t_{13}, t_{24}, t_{14}, t_{23}, t = abcd) \in \mathbb{F}_p^7$ defines a point on an algebraic variety $\mathcal{C}$ over $\mathbb{F}_p$ defined by the following equations:

$$(t_{12}^2 - 1)(t_{34}^2 - 1) = t$$
$$(t_{13}^2 - 1)(t_{24}^2 - 1) = t$$
$$(t_{14}^2 - 1)(t_{23}^2 - 1) = t.$$

Conversely, the points $(\pm t_{12}, \pm t_{34}, \pm t_{13}, \pm t_{24}, \pm t_{14}, \pm t_{23}, t) \in \mathbb{F}_p^7$ on $\mathcal{C}$ determine two ordered Diophantine quadruples $\pm(a, b, c, d)$, provided that the elements a, b, c and d are $\mathbb{F}_p$-rational, distinct and non-zero. Here, we take $a = \sqrt{(t_{12}^2 - 1)(t_{13}^2 - 1)/(t_{23}^2 - 1)}$ to be any square root, while b, c and d are defined using identities $ab + 1 = t_{12}^2$, $ac + 1 = t_{13}^2$ and $ad + 1 = t_{14}^2$. It follows from this definition and the equations defining $\mathcal{C}$ that $bc + 1 = t_{23}^2$, $bd + 1 = t_{24}^2$ and $cd + 1 = t_{34}^2$. Also, if only one element of quadruple is $\mathbb{F}_p$-rational, then all the elements are $\mathbb{F}_p$-rational.

The projection $(t_{12}, t_{34}, t_{13}, t_{24}, t_{14}, t_{23}, t) \mapsto t$ defines a fibration of $\mathcal{C}$ over the projective line, and the generic fiber is a cube of $\mathcal{D}_t : (x^2 - 1)(y^2 - 1) = t$. Any point on $\mathcal{C}$ corresponds to the three points $Q_1 = (t_{12}, t_{34})$, $Q_2 = (t_{13}, t_{24})$ and $Q_3 = (t_{14}, t_{23})$ on $\mathcal{D}_t$. The elements of a

quadruple corresponding to these three points are distinct if and only if no two of these points can be transformed from one to another by changing signs and switching coordinates (e.g. for the points (t_{12}, t_{34}), $(-t_{34}, t_{12})$ and (t_{14}, t_{23}), we have that $a = d$).

The curve $\mathcal{D}_t$ for $t \in \mathbb{F}_p$ is birationally equivalent to the curve

$$E_t : V^2 = U^3 - 2(t-2)U^2 + t^2U.$$

The map is given by $U = 2(x^2-1)y + 2x^2 - (2-t)$, and $V = 2Ux$. The family E_t over the t-line together with $R = (t, 2t)$, the point of order 4, is the universal elliptic curve over the modular curve $X_1(4)$ (we identify $\mathbb{P}^1$ with $X_1(4)$ such that cusps of $X_1(4)$ correspond to $t = 0, 1$ and ∞). It is easy to see that the affine $\mathbb{F}_p$-points on the curve $\mathcal{D}_t$ are in $1-1$ correspondence with the set $\tilde{E}_t(\mathbb{F}_p) := E_t(\mathbb{F}_p) \setminus \{\mathcal{O}, R, 2R, 3R\}$.

If $t \neq 0, 1$ the curve E_t is an elliptic curve, so in our analysis of Diophantine quadruples we will naturally distinguish two cases $t = 1$ and $t \neq 0, 1$ (note that $t = 0$ would imply that one of the elements in quadruple $\{a, b, c, d\}$ is zero).

If $t = 1$ then there is a singular point $(-1, 0)$ on the curve $E_1 : V^2 = U(U+1)^2$ which corresponds to the point $(0, 0)$ on $\mathcal{D}_1$.

If $Q \in \tilde{E}_t(\mathbb{F}_p)$ is the nonsingular point that corresponds to the point $(x, y) \in \mathcal{D}_t(\mathbb{F}_p)$, then a direct calculation shows that the points $-Q$ and $Q + R$ correspond to the points $(-x, y)$ and $(y, -x)$ respectively. Hence the following lemma follows.

Lemma 2. *Let $t \in \mathbb{F}_p^\times$. The triple $(Q_1, Q_2, Q_3) \in \tilde{E}_t(\mathbb{F}_p)^3$ corresponds to the quadruple whose elements are not distinct if and only if there are two nonsingular points, Q_i and Q_j with $i \neq j$ such that $Q_i = \pm Q_j + kR$, where $k \in \{0, 1, 2, 3\}$ or if at least two points in the triple are singular.*

A short calculation shows that for the point $(U, V) \in \tilde{E}_t(\mathbb{F}_p)$ corresponding to $(x, y) \in \mathcal{D}_t$ we have

$$x^2 - 1 = \left(\frac{V}{2U}\right)^2 - 1 = U\left(\frac{U-t}{2U}\right)^2 =: f((U, V)).$$

Since

$$a^2 = \frac{f(Q_1)f(Q_2)f(Q_3)}{t} \equiv U(Q_1)U(Q_2)U(Q_3)t \equiv U(Q_1)U(Q_2)U(Q_3)U(R) \pmod{\mathbb{F}_p^{\times 2}}$$

for the rationality of a it is enough to prove that $U(Q_1)U(Q_2)U(Q_3)U(R)$ is a square in $\mathbb{F}_p^{\times 2}$.

If $t = 1$ and $Q = (U, V) \in \tilde{E}_1(\mathbb{F}_p)$ is a nonsingular point, then $f(Q) = \frac{V^2}{(U+1)^2}\frac{(U-1)^2}{(2U)^2}$ is always a square in $\mathbb{F}_p$, hence the triple $(Q_1, Q_2, Q_3) \in \tilde{E}_1(\mathbb{F}_p)^3$ of distinct points corresponds to the quadruple whose elements are $\mathbb{F}_p$-rational if and only if -1 is a square in $\mathbb{F}_p$ (since -1 is U-coordinate of the singular point) or if all the points Q_i are nonsingular.

For $t \neq 0, 1$, since $(0, 0) \in E_t(\mathbb{F}_p)$ is a point of order two, there is an elliptic curve E_t' defined over $\mathbb{F}_p$ and 2-isogeny $\phi' : E_t \to E_t'$ such that $\ker \phi' = \langle (0, 0) \rangle$. Denote by $\phi : E_t' \to E_t$ the dual isogeny of ϕ', and by $\Gamma_t := \phi(E_t'(\mathbb{F}_p)) \subset E_t(\mathbb{F}_p)$ index two subgroup of $E_t(\mathbb{F}_p)$ consisting of points $\{\mathcal{O}, 2R\}$ and of points P such that $U(P)$ is a nonzero square (see the proof of the following lemma).

Lemma 3. *If $t \neq 0, 1$ then the triple $(Q_1, Q_2, Q_3) \in \tilde{E}_t(\mathbb{F}_p)^3$ corresponds to the quadruple whose elements are $\mathbb{F}_p$-rational, if and only if*

$$Q_1 + Q_2 + Q_3 + R \in \Gamma_t.$$

Proof. There is an injective descent homomorphism $\delta_\phi : E_t(\mathbb{F}_p)/\phi(E_t'(\mathbb{F}_p)) \to H^1(\mathbb{F}_p, E_t'[\phi]) \cong \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$ (see Section 2 of [MS10]), which maps point $(U,V) \mapsto U$ if $U \neq 0$, and points $2R = (0,0), \mathcal{O} \mapsto 1$. Hence we see that $\Gamma_t = \phi(E_t'(\mathbb{F}_p))$ consists of points P such that $U(P)$ is a square and the point $\mathcal{O}$.

It follows that

$$U(Q_1)U(Q_2)U(Q_3)U(R) \equiv \delta_\phi(Q_1+Q_2+Q_3+R) \pmod{\mathbb{F}_p^{\times 2}},$$

hence the claim follows. □

We call a triple $(Q_1,Q_2,Q_3) \in \tilde{E}_t(\mathbb{F}_p)^3$ *admissible* if it corresponds to a Diophantine quadruple. It follows from Lemma 2 and Lemma 3 that this holds if and only if the following is true

a) $t \neq 0$,
b) there are no two nonsingular points Q_i and Q_j with $i \neq j$ such that $Q_i = \pm Q_j + kR$ for some $k \in \{0,1,2,3\}$ and there not two singular points Q_i and Q_j with $i \neq j$.
c) if $t \neq 0,1$ then $Q_1+Q_2+Q_3+R \in \Gamma_t$ or if $t=1$ then all Q_i's are nonsingular or -1 is a square in $\mathbb{F}_p$.

3. Counting admissible triples

The main idea of this paper is to count the number $N^{(4)}(p)$ of Diophantine quadruples over $\mathbb{F}_p$, by counting the admissible triples (Q_1,Q_2,Q_3).

Since each pair of ordered Diophantine quadruples $\pm(a,b,c,d)$ correspond to several admissible triples, we count each admissible triple (Q_1,Q_2,Q_3) with certain weight $w = w(Q_1,Q_2,Q_3)$.

We choose w such that $\frac{2}{w}$ is equal to the number of admissible triples that correspond to the same ordered pair of Diophantine quadruples as (Q_1,Q_2,Q_3).

Thus, if for $t \in \mathbb{F}_p\backslash\{0,1\}$, we denote by

$$W(t) = \frac{1}{4!} \sum_{(Q_1,Q_2,Q_3)} w(Q_1,Q_2,Q_3),$$

where the sum is over all admissible triples $(Q_1,Q_2,Q_3) \in E_t(\mathbb{F}_p)^3$, then $W(t)$ is equal to the number of Diophantine quadruples $\{a,b,c,d\}$ with $abcd = t$.

Diophantine quadruples with $abcd = 1$ (corresponding to the singular fiber $\mathcal{D}_1$) will be counted separately (see Proposition 7) - we denote their number by $W(1)$. Our goal is to evaluate the sum

$$N^{(4)}(p) = \sum_{t \in \mathbb{F}_p^\times} W(t).$$

For every $Q \in \tilde{E}_t(\mathbb{F}_p)$, denote by $[Q]$ the set $\{Q+kR, -Q+kR : k \in \{0,1,2,3\}\}$. We call such a set the class of Q. Note that $\#[Q] = 8$, unless $[Q]$ contains a point of order 2 (different than $2R = (0,0)$) or a point Q' such that $2Q' = \pm R$, in which case $\#[Q] = 4$. Note that for an admissible triple (Q_1,Q_2,Q_3) the classes $[Q_1], [Q_2]$ and $[Q_3]$ are disjoint.

LEMMA 4. *Let (Q_1,Q_2,Q_3) be an admissible triple. If there exists $k \in \{1,2,3\}$ such that $[Q_k] = [T]$ for some $T \in E_t(\mathbb{F}_p)[2]\backslash\{2R\}$, then $w(Q_1,Q_2,Q_3) = 2^{-4}$, otherwise $w(Q_1,Q_2,Q_3) = 2^{-5}$.*

Proof. If we fix the pair of ordered Diophantine quadruples $\pm(a,b,c,d)$, then for each choice of the signs $\pm t_{ij}$ there is one admissible triple (Q_1,Q_2,Q_3) corresponding to it. Since $t \neq 1$, at most

one t_{ij} can be equal to zero, and this will happen if and only if the class of one of the points Q_k contains a point of order two different from $2R$ (since if Q_k corresponds to (x,y) in $\mathcal{D}_t$, then $-Q_k, Q_k+2R$ and $-Q_k+2R$ correspond to $(-x,y),(-x,-y)$ and $(x,-y)$ respectively). In this case $w=2^{-4}$, otherwise $w=2^{-5}$. □

For $t\in\mathbb{F}_p, t\neq 0,1$, denote by $P(t)=\#E_t(\mathbb{F}_p)$. In the rest of the section, we will express $W(t)$ as a polynomial in $Q(t):=\frac{P(t)}{4}$ using following counting idea.

Let $\mathcal{C}=\{C_1,\dots,C_n\}$ be the set of all classes $[Q]\subset\tilde{E}_t(\mathbb{F}_p)$. Define $w(C)=1$ for all classes C except $w([T])=2$, where $[T]$ is the class that contains a point of order 2 different from $2R$ (if such element exists). Then for $t\neq 0,1$, it follows from Lemma 4 that $4!\cdot W(t)$ is equal to

$$\frac{3!}{2^5}\sum_{\{C,C',C''\}\subset\mathcal{C}} w(C)w(C')w(C'')\#\{(Q_1,Q_2,Q_3)\in C\times C'\times C'': Q_1+Q_2+Q_3+R\in\Gamma_t\},$$

where the sum is over three element subsets of $\mathcal{C}$. To evaluate this formula we will need some additional information about the structure of $E_t(\mathbb{F}_p)$.

In what follows, T always denotes a 2-torsion point in $E_t(\mathbb{F}_p)$ different from $2R$ and Q denotes a point in $E_t(\mathbb{F}_p)$ such that $2Q=R$ (if these points exist). We denote by S_j, S_j' and S_j'' sets of $t\neq 0,1$ such that $E_t(\mathbb{F}_p)$ has respective properties:

S_0: T and Q both do not exist and $R\notin\Gamma_t$,
S_1': T exists, but Q does not and $R\notin\Gamma_t$,
S_1'': T exists, but Q does not and $R\in\Gamma_t$,
S_2': T does not exist, but Q does and $Q\notin\Gamma_t$,
S_2'': T does not exist, but Q does and $Q\in\Gamma_t$,
S_3: T and Q both exist and $Q\in\Gamma_t, Q+T\notin\Gamma_t$,
S_3': T and Q both exist and $Q, Q+T\notin\Gamma_t$,
S_3'': T and Q both exist and $Q, Q+T\in\Gamma_t$.

Proposition 5. *Let p be an odd prime and $t\in\mathbb{F}_p, t\neq 0,1$. Then t is an element of one set defined above. The expression for $4!\cdot W(t)$ in terms of $Q(t)=\#E_t(\mathbb{F}_p)/4$ is given in the following table (the sets not included in the table are empty).*

$p\equiv 1 \pmod 4$	$4!\cdot W(t)$
$t\in S_0$	$Q(t)^3-9Q(t)^2+23Q(t)-15$
$t\in S_1'$	$Q(t)^3-6Q(t)^2+8Q(t)$
$t\in S_1''$	$Q(t)^3-6Q(t)^2+8Q(t)$
$t\in S_2'$	$Q(t)^3-9Q(t)^2+32Q(t)-36$
$t\in S_2''$	$Q(t)^3-9Q(t)^2+32Q(t)-48$
$t\in S_3'$	$Q(t)^3-6Q(t)^2+14Q(t)$
$t\in S_3''$	$Q(t)^3-6Q(t)^2+14Q(t)-24$
$p\equiv 3 \pmod 4$	$4!\cdot W(t)$
$t\in S_0$	$Q(t)^3-9Q(t)^2+23Q(t)-15$
$t\in S_1'$	$Q(t)^3-6Q(t)^2+8Q(t)$
$t\in S_1''$	$Q(t)^3-6Q(t)^2+20Q(t)-24$
$t\in S_2'$	$Q(t)^3-9Q(t)^2+32Q(t)-36$
$t\in S_2''$	$Q(t)^3-9Q(t)^2+32Q(t)-48$
$t\in S_3$	$Q(t)^3-6Q(t)^2+26Q(t)-48$

For the proof of this proposition, we will need the following technical result.

PROPOSITION 6. *Let p be an odd square, and $t \neq 0, 1$ in $\mathbb{F}_p$ be such that $E_t(\mathbb{F}_p)[2] \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Denote by $T \in E_t(\mathbb{F}_p)[2]$ a point of order two, $T \neq 2R$. The following are equivalent*

i) $U(T)$ is a square,

ii) $p \equiv 1 \pmod 4$.

Proof. To prove equivalence between $i)$ and $ii)$, note that the U-coordinates of the points of order two satisfy $U(U^2+(4-2t)U+t^2)=0$. In particular, $U(T) = t-2\pm 2\sqrt{1-t} = -(\pm\sqrt{1-t}-1)^2$ is a square if and only if $\left(\frac{-1}{p}\right) = 1$ (note that $U(T) \in \mathbb{F}_p$ implies $\sqrt{1-t} \in \mathbb{F}_p$). □

Proof of Proposition 5. Recall the formula

$$4!W(t) = \frac{3!}{2^5} \sum_{\{C,C',C''\}\subset\mathcal{C}} w(C)w(C')w(C'')\#\{(Q_1,Q_2,Q_3) \in C\times C'\times C'' : Q_1+Q_2+Q_3+R \in \Gamma_t\}. \tag{1}$$

First we consider the case when $R \notin \Gamma_t$ (which implies that Q does not exist), i.e. $t \in S_0 \cup S_1'$. Since the only possible class of size 4 is $[T]$, we always have $w(C)\#C = 8$. It follows that

$$4!W(t) = \frac{3!}{2^5} \sum_{\{C,C',C''\}\subset\mathcal{C}} \frac{1}{2} w(C)\#Cw(C')\#C'w(C'')\#C'' = \frac{3!}{2^5} \sum_{\{C,C',C''\}\subset\mathcal{C}} 2^8,$$

since half of the triples (Q_1,Q_2,Q_3) will have the property that $Q_1+Q_2+Q_3 \in \Gamma_t$ (note that for every $P \in \tilde{E}_t(\mathbb{F}_p)$ precisely one of P and $P+R$ is an element of Γ_t since by two-isogeny descent homomorphism we have that $U(P+R) \equiv U(P)U(R) \pmod{\mathbb{F}_p^{\times 2}}$ - see the proof of Lemma 3). It follows that $4!W(t) = 2^3 \cdot 3!\binom{\#\mathcal{C}}{3}$. Since $\#\mathcal{C} = \frac{P(t)-4}{8} = \frac{Q(t)-1}{2}$ if $\#E_t(\mathbb{F}_p)[2] = 2$ (case $t \in S_0$), and $\#\mathcal{C} = \frac{P(t)}{8} = \frac{Q(t)}{2}$ otherwise (case $t \in S_1'$) the formula in these two cases follows.

In all other cases, when $R \in \Gamma_t$, the term $w(C)w(C')w(C'')\#\{(Q_1,Q_2,Q_3) \in C\times C'\times C'' : Q_1+Q_2+Q_3+R \in \Gamma_t\}$ is equal either zero or $w(C)\#Cw(C')\#C'w(C'')\#C''$ depending on whether an odd or even number of the classes is contained in Γ_t (since $U(Q_1+R) \equiv U(Q_1) \pmod{\mathbb{F}_p^{\times 2}}$) each class $[Q_1]$ is either contained in Γ_t or in its complement). If we denote by $\mathcal{C}_+$ and $\mathcal{C}_-$ the sets of classes contained in Γ_t and its complement respectively, then the sum in (1) is effectively over three-element subsets of $\mathcal{C}_+$ and over combinations of one element in $\mathcal{C}_+$ and two elements in $\mathcal{C}_-$. A derivation of the formula for $W(t)$ then boils down to the simple combinatorial analysis of the sets $\mathcal{C}_+$ and $\mathcal{C}_-$.

We will illustrate this method in three cases.

$t \in S_1''$: If $p \equiv 1 \pmod 4$ then Proposition 6 implies that $T \in \Gamma_t$. There are $b_1 = \frac{P(t)-16}{16}$ eight-element classes $[Q_i]$ in $\mathcal{C}_+$ together with a four-element class $[T]$ (and the class $[R]$ which we don't count), and $b_2 = \frac{P(t)}{16}$ eight-element classes $[Q_i]$ in $\mathcal{C}_-$. Note that since Γ_t is index two subgroup of $E_t(\mathbb{F}_p)$ the total number of elements of the union of all the classes in $\mathcal{C}_+$ is equal to $P(t)/2$. Since for all the classes $[C]$ we have $w(C)\#C = 2^3$, following the counting procedure outlined above (i.e. we choose any three classes from $\mathcal{C}_+$ or one class from $\mathcal{C}_+$ and two classes from $\mathcal{C}_-$) we obtain

$$4!W(t) = \frac{3!}{2^5}\binom{b_1+1}{3}(2^3)^3 + \frac{3!}{2^5}(b_1+1)\binom{b_2}{2}(2^3)^3$$
$$= \frac{P(t)(P(t)-8)(P(t)-16)}{64} = Q(t)^3 - 6Q(t)^2 + 8Q(t).$$

If $p \equiv 3 \pmod 4$ then Proposition 6 implies that $T \notin \Gamma_t$. There are $b = \frac{P(t)-8}{16}$ eight-element classes $[Q_i]$ in $\mathcal{C}_+$, and the same number of eight-element classes $[Q_i]$ in $\mathcal{C}_-$ (together with the class $[T]$). Hence,

$$4!W(t) = \frac{3!}{2^5}\binom{b}{3}(2^3)^3 + \frac{3!}{2^5}b\binom{b+1}{2}(2^3)^3$$
$$= \frac{1}{64}(P(t)-8)(P(t)^2 - 16P(t) + 192) = Q(t)^3 - 6Q(t)^2 + 20Q(t) - 24.$$

$t \in S_2'$: There are $b = \frac{P(x)-8}{16}$ eight-element classes in both $\mathcal{C}_+$ and $\mathcal{C}_-$, while $\mathcal{C}_-$ contains a four-element class $[Q]$ (for which $w(Q)\#Q = 4$). Hence,

$$4!W(t) = \frac{3!}{2^5}\left(\binom{b}{3}(2^3)^3 + b\cdot b\cdot 1(2^3)^2\cdot(2^2) + b\binom{b}{2}(2^3)^3\right)$$
$$= \frac{(P(t)-8)(P(t)^2 - 28P(t) + 288)}{64} = Q(t)^3 - 9Q(t)^2 + 32Q(t) - 36.$$

$t \in S_3'''$: In this case we have three four-element classes: $[Q], [T]$ and $[Q+T]$. Since $Q \notin \Gamma_t$ and $Q+T \in \Gamma_t$ it follows that $T \notin \Gamma_t$, hence Proposition 6 implies that $p \equiv 3 \pmod 4$. There are $b = \frac{P(t)-16}{16}$ eight-element classes in both $\mathcal{C}_+$ and $\mathcal{C}_-$. We calculate (recall that $w(C)\#C = 8$ for all the classes $[C]$ except $[T+Q]$ and $[Q]$)

$$4!W(t) = \frac{3!}{2^5}\left(\binom{b}{3}(2^3)^3 + 1\cdot\binom{b}{2}2^2\cdot(2^3)^2 + b\cdot 1\cdot(b+1)2^3\cdot 2^2\cdot 2^3\right.$$
$$\left. + 1\cdot 1\cdot(b+1)2^2\cdot 2^2\cdot 2^3 + b\binom{b+1}{2}(2^3)^3 + 1\cdot\binom{b+1}{2}2^2\cdot(2^3)^2\right)$$
$$= \frac{P(t)^3 - 24P(t)^2 + 416P(t) - 3072}{64} = Q(t)^3 - 6Q(t)^2 + 26Q(t) - 48$$

The other cases are proved in the similar way.

Note that the case when $R \in \Gamma_t$ and both T and Q do not exist can not occur since it would imply that $\#\Gamma_t \equiv 0 \pmod 4$, or that $P(t)$ is divisible by 8 which is not true since there is only one class $[R]$ of size 4. □

3.1 Putting everything together

Now for $p \equiv 1 \pmod 4$ we have

$$\begin{aligned}4! \sum_{t\neq 0,1} W(t) = &\sum_{t\in S_0}(Q(t)^3 + 9Q(t)^2 + 23Q(t) - 15)\\ &+ \sum_{t\in S_1}(Q(t)^3 - 6Q(t)^2 + 8Q(t))\\ &+ \sum_{t\in S_2'}(Q(t)^3 - 9Q(t)^2 + 32Q(t) - 36)\\ &+ \sum_{t\in S_2''}(Q(t)^3 - 9Q(t)^2 + 32Q(t) - 48)\\ &+ \sum_{t\in S_3'}(Q(t)^3 - 6Q(t)^2 + 14Q(t))\\ &+ \sum_{t\in S_3''}(Q(t)^3 - 6Q(t)^2 + 14Q(t) - 24),\end{aligned}$$

where we defined $S_1 := S_1' \cup S_1''$ (since the formula for $W(t)$ in those two cases is the same). We have the similar formula when $p \equiv 3 \pmod 4$.

For an odd prime p we define the following sets:

$$\begin{aligned}T_1 &= \left\{t \in \mathbb{F}_p^\times \setminus \{1\} : \#E_t(\mathbb{F}_p)[2] = 4\right\},\\ T_2 &= \left\{t \in \mathbb{F}_p^\times \setminus \{1\} : \exists Q \in E_t(\mathbb{F}_p) : 2Q = R\right\},\\ T_3 &= T_1 \cap T_2.\end{aligned}$$

The reason for introducing sets T_i is that we can evaluate sums of the form $\sum_{t\in T_i} Q(t)^j$ by relating them to the modular forms (of weight $j+2$) on modular curves $X(2,4), X_1(8)$ and $X(2,8)$.

One can check that if $p \equiv 1 \pmod 4$ then

$$T_1 = S_1 \cup S_3' \cup S_3'', \qquad T_2 = S_2' \cup S_2'' \cup S_3' \cup S_3'', \quad T_3 = S_3' \cup S_3'',$$

and so we have

$$\begin{aligned}4! \sum_{t\neq 0,1} W(t) = &\sum_{t\neq 0,1}(Q(t)^3 - 9Q(t)^2 + 23Q(t) - 15) + \sum_{t\in T_1}(3Q(t)^2 - 15Q(t) + 15)\\ &+ \sum_{t\in T_2}(9Q(t) - 21) - \sum_{t\in T_3}(3Q(t) - 21) - 12\#S_2'' - 24\#S_3''.\end{aligned}$$

If $p \equiv 3 \pmod 4$ then

$$T_1 = S_1' \cup S_1'' \cup S_3, \qquad T_2 = S_2' \cup S_2'' \cup S_3, \quad T_3 = S_3,$$

and we have

$$\begin{aligned}4! \sum_{t\neq 0,1} W(t) = &\sum_{t\neq 0,1}(Q(t)^3 - 9Q(t)^2 + 23Q(t) - 15) + \sum_{t\in T_1}(3Q(t)^2 - 3Q(t) + 3)\\ &+ \sum_{t\in T_2}(9Q(t) - 21) - \sum_{t\in T_3}(3Q(t) + 3) - 12\sum_{t\in S_1'} Q(t) - 12\#S_2'' + 12(\#S_1' - \#S_1'' - \#S_3).\end{aligned}$$

These formulas will be further simplified in the Section 5.

3.2 Calculating $W(1)$

The curve $\mathcal{D}_1 : (x^2-1)(y^2-1) = 1$ is birationally equivalent to the genus zero curve $E_1 : S^2 = U(U+1)^2$. Analysis similar (but easier) to the one in Section 2 yields the following proposition.

Proposition 7.

$$4! \cdot W(1) = \begin{cases} \frac{(p-9)(p^2-18p+113)}{32}, & \text{if } p \equiv 1 \pmod 8, \\ \frac{(p-3)(p-11)(p-19)}{32}, & \text{if } p \equiv 3 \pmod 8, \\ \frac{(p-5)(p-9)(p-13)}{32}, & \text{if } p \equiv 5 \pmod 8, \\ \frac{(p-7)(p-11)(p-15)}{32}, & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

4. Families of universal elliptic curves and ℓ-adic representations

4.1 Modular curves and cusps

For $M, N \geqslant 1$, $M|N$, we denote by $Y(M,N)$ the quotient of the upper half plane by the congruence subgroup $\Gamma_1(N) \cap \Gamma^0(M)$. Here $\Gamma^0(M) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right) \pmod M \right\}$. As a modular curve (irreducible, connected and defined over $\mathbb{Q}(\zeta_M)$) $Y(M,N)$ parametrizes elliptic curves E together with the points P and Q of order M and N, such that P and Q generate subgroup of order MN and the Weil pairing e_M between the points P and $\frac{N}{M}Q$ is equal to the fixed primitive M-th root of unity, i.e. $e_M(P, \frac{N}{M}Q) = e^{2\pi i/M}$. We denote by $X(M,N)$ the compactification of $Y(M,N)$. For more information on modular curves $Y(M,N)$ see Section 2 in [Kato04].

In Section 5, we will need to know the number of $\mathbb{F}_p$-rational cusps on modular curves $X_1(8)_{\mathbb{F}_p}, X(2,4)_{\mathbb{F}_p}$ and $X(2,8)_{\mathbb{F}_p}$. Following [BN16, Section 2], we briefly explain how to calculate the field of definition of cusps on $X(M,N)$.

Let r be a divisor of N. The cusps of $X(M,N)$ represented by the points $(a:b) \in \mathbb{P}^1(\mathbb{Q})$, where a, b are co-prime integers with $\gcd(b,N) = r$, all have the same field of definition, $\mathbb{Q}(\zeta_M) \leqslant F_r \leqslant \mathbb{Q}(\zeta_N)$. If we canonically identify $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ with $(\mathbb{Z}/N\mathbb{Z})^\times$, then F_r is the fixed field of the group H_r acting on $\mathbb{Q}(\zeta_N)$, where $H_r = H_r^0 := \{s \in (\mathbb{Z}/N\mathbb{Z})^\times : s \equiv 1 \pmod{\mathrm{lcm}(M, N/r)}\}$, if $\gcd(Mr, N) > 2$, and $H_r = H_r^0 \cdot \{\pm 1\}$ otherwise.

It follows immediately that all four cusps of $X(2,4)$ are $\mathbb{Q}$-rational (i.e. $c(2,4) = 4$), and that the number $c(2,8)$ of $\mathbb{F}_p$-rational cusps of $X(2,8)_{\mathbb{F}_p}$ is equal to

$$c(2,8) = \begin{cases} 10, & \text{if } p \equiv 1 \pmod 8, \\ 4, & \text{if } p \equiv 3 \pmod 8, \\ 6, & \text{if } p \equiv 5 \pmod 8, \\ 8, & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

Moreover, the number of $\mathbb{F}_p$-rational cusps on modular curve $X_1(8)_{\mathbb{F}_p}$ is equal to

$$c(8) = \begin{cases} 6, & \text{if } p \equiv 1, 7 \pmod 8, \\ 4, & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$$

The curves $X_1(4), X(2,4), X_1(8)$ and $X(2,8)$ have genus zero.

4.2 Modular forms

Here we collect some facts about the spaces of modular forms related to the modular curves from the previous subsection. They can be checked using Sage [SAGE] and LMFDB database [LMFDB].

Proposition 8. *Denote by T_p the p-th Hecke operator acting on the space of cusp forms $S_3(\Gamma_1(8)\cap\Gamma^0(2))$. We have*

a) $\dim S_3(\Gamma_1(4)) = \dim S_4(\Gamma_1(4)) = 0$ *and* $S_5(\Gamma_1(4)) = \mathbb{C}\cdot f_4(\tau)$,
b) $\dim S_3(\Gamma_1(8)\cap\Gamma^0(2)) = 3$ *and* $Trace(T_p) = 2b(p) + c(p)$,
c) $S_3(\Gamma_1(8)) = \mathbb{C}\cdot f_1(\tau)$,
d) $S_3(\Gamma_1(4)\cap\Gamma^0(2)) = 0$ *and* $S_4(\Gamma_1(4)\cap\Gamma^0(2)) = \mathbb{C}\cdot f_3(\tau)$.

Modular forms $f_1(\tau), f_2(\tau)$ and $f_4(\tau)$ are CM forms, and their Fourier coefficients are given in the following proposition. For some standard facts about CM modular forms see [Ono03, p.9].

Proposition 9. *Let p be an odd prime and $q = e^{2\pi i\tau}$. We have*

b) $f_1(\tau) = \eta^2(\tau)\eta(2\tau)\eta(4\tau)\eta^2(8\tau) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{2n})(1-q^{4n})(1-q^{8n})^2$, *and*

$$b(p) = \begin{cases} 2(x^2-2y^2), & \text{if } p\equiv 1,3 \pmod 8 \text{ and } p = x^2+2y^2 \\ 0, & \text{if } p\equiv 5,7 \pmod 8, \end{cases}$$

c) $f_2(\tau) = \eta^6(4\tau) = q\prod_{n=1}^{\infty}(1-q^{4n})^6$, *and*

$$c(p) = \begin{cases} \pm 2(x^2-4y^2), & \text{if } p\equiv 1 \pmod 4 \text{ and } p = x^2+4y^2 \\ 0, & \text{if } p\equiv 3 \pmod 4, \end{cases}$$

d) $f_3(\tau) = \eta^4(2\tau)\eta^4(4\tau) = q\prod_{n=1}^{\infty}(1-q^{2n})^4(1-q^{4n})^4$,
e) $f_4(\tau) = \eta^4(\tau)\eta^2(2\tau)\eta^4(4\tau) = q\prod_{n=1}^{\infty}(1-q^n)^4(1-q^{2n})^2(1-q^{4n})^4$, *and*

$$e(p) = \begin{cases} 2p^2-16x^2y^2, & \text{if } p\equiv 1 \pmod 4 \text{ and } p = x^2+y^2 \\ 0, & \text{if } p\equiv 3 \pmod 4. \end{cases}$$

4.3 Families of universal elliptic curves

Let E^1, E^2, E^3 and E^4 be elliptic surfaces fibered over the modular curves $X_1(4)$, $X(2,4)$, $X_1(8)$ and $X(2,8)$ defined by affine equations (given with the sections of the corresponding orders):

$$E^1 : Y^2 = X(X^2 - 2(t_1-2)X + t_1^2), \quad P_1 = [t_1, 2t_1]; 4P_1 = \mathcal{O}$$

$$E^2 : Y^2 = X(X + t_2^2 - 2t_2 + 1)(X + t_2^2 + 2t_2 + 1),$$
$$P_2 = [1-t_2^2, 2(1-t_2^2)], \quad T_2 = [-t_2^2+2t_2-1, 0]; 4P_2 = 2T_2 = \mathcal{O}$$

$$E^3 : Y^2 = X\left(X^2 - 2(t_3^4 - 2t_3^2 - 1) + (t_3-1)^4(t_3+1)^4\right),$$
$$Q_3 = [(t_3-1)(t_3+1)^3, 2t_3(t_3-1)(t_3+1)^3]; 8Q_3 = \mathcal{O}$$

$$E^4 : Y^2 = X\left(X + \frac{64t_4^4}{(t_4^2+1)^4}\right)\left(X + \frac{4(t_4-1)^4(t_4+1)^4}{(t_4^2+1)^4}\right),$$
$$Q_4 = \left[\frac{-16t_4(t_4-1)(t_4+1)^3}{(t_4^2+1)^4}, \frac{32t_4(t_4-1)(t_4+1)^3(t_4^2-2t_4-1)}{(t_4^2+1)^5}\right], T_4 = \left[-\frac{64t_4^4}{(t_4^2+1)^4}, 0\right];$$
$$8Q_4 = 2T_4 = \mathcal{O}$$

together with the maps

$$h_1 : E^1 \to X_1(4) \quad (X, Y, t_1) \mapsto t_1,$$
$$h_2 : E^2 \to X(2,4) \quad (X, Y, t_2) \mapsto t_2,$$
$$h_3 : E^3 \to X_1(8) \quad (X, Y, t_3) \mapsto t_3,$$
$$h_4 : E^4 \to X(2,8) \quad (X, Y, t_4) \mapsto t_4.$$

Here we identify modular curves $X_1(4)$, $X(2,4)$, $X_1(8)$, and $X(2,8)$ with $\mathbb{P}^1$ using parameters t_1, t_2, t_3, and t_4.

We have the natural maps

$$g_2 : X(2,4) \to X_1(4), \quad (E, T_2, P_2) \mapsto (E, P_2), \quad t_1 = 1 - t_2^2$$
$$g_3 : X_1(8) \to X_1(4), \quad (E, Q_3) \mapsto (E, 2Q_3), \quad t_1 = (t_3^2 - 1)^2$$
$$g_4 : X(2,8) \to X_1(4), \quad (E, T_4, Q_4) \mapsto (E, 2Q_4), \quad t_1 = \frac{16t_4^2(t_4-1)^2(t_4+1)^2}{(t_4^2+1)^4}.$$

Note that the maps g_2 and g_4 are Galois (e.g. $Aut(g_2)$ is generated by the map $(E, T_2, P_2) \mapsto (E, T_2 + 2P_2, P_2)$, while g_3 is not (its Galois closure is given by g_4).

Elliptic surfaces E^1, E^2, E^3 and E^4 are universal elliptic curves over the modular curves $X_1(4), X(2,4), X_1(8)$ and $X(2,8)$ respectively (for the universality, it is enough to check that for each i the degree of j-invariant $j(E^i)$ is equal to the index of the corresponding subgroup in $\mathrm{SL}_2(\mathbb{Z})$).

4.4 Compatible families of ℓ-adic Galois representations of $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

To each of these elliptic surfaces and to every positive integer k, we can associate two compatible families of ℓ-adic Galois representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. To ease notation, we denote by Γ_j, for $j = 1, 2, 3, 4$, groups $\Gamma_1(4), \Gamma(2,4), \Gamma_1(8)$ and $\Gamma(2,8)$ respectively, and by $X(\Gamma_j)$ the corresponding modular curve.

We define the representation $\rho_{j,\ell}^k$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ as follows. Let $X(\Gamma_j)^0$ be the complement in $X(\Gamma_j)$ of the cusps. Denote by i the inclusion of $X(\Gamma_j)^0$ into $X(\Gamma_j)$, and by $h_j' : E^{j,0} \to X(\Gamma_j)^0$ the restriction of elliptic surface h_j to $X(\Gamma_j)^0$. For a prime ℓ we obtain a sheaf

$$\mathcal{F}_\ell^j = R^1 h_{j*}' \mathbb{Q}_\ell$$

on $X(\Gamma_j)^0$, and also a sheaf $i_* \mathrm{Sym}^k \mathcal{F}_\ell^j$ on $X(\Gamma_j)$ (here $\mathbb{Q}_\ell$ is the constant sheaf on the elliptic surface $E^{j,0}$, and R^1 is derived functor). The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the $\mathbb{Q}_\ell$-space

$$W_{k,\ell}^j = H_{et}^1(X(\Gamma_j) \otimes \overline{\mathbb{Q}}, i_* \mathrm{Sym}^k \mathcal{F}_\ell^j)$$

defines ℓ-adic representation $\rho_{j,\ell}^k$ which is pure of weight $k+1$.

The second family, $\tilde{\rho}_{j,\ell}^k$, is ℓ-adic realization of the motive associated to the spaces of cusp forms $S_{k+2}(\Gamma_j)$. For the construction see [Sch85, Section 5].

Similarly as in [ALL08, Section 3], since the elliptic surface E^j is the universal elliptic curve over the modular curve $X(\Gamma_j)$, we can argue that these two representations are isomorphic, i.e. $\rho_{j,\ell}^k \sim \tilde{\rho}_{j,\ell}^k$. In particular, we will frequently use the following proposition.

PROPOSITION 10. *Let $k \geqslant 1$ be an integer and $j \in \{1,2,3,4\}$. Denote by B the set of normalized Hecke eigenforms in $S_{k+2}(\Gamma_j)$. For every odd prime $\ell \neq p$ we have*

$$Trace(\rho_{j,\ell}^k(Frob_p)) = \sum_{f \in B} a_f(p),$$

where $a_f(p)$ is the p-th Fourier coefficient of the eigenform f, and $Frob_p$ is a geometric Frobenius at p.

4.5 Traces of Frobenius

To simplify notation, denote $\mathcal{F} = R^1 h'_{j*}\mathbb{Q}_\ell$ and $W = H^1_{et}(X(\Gamma_j) \otimes \overline{\mathbb{Q}}, i_*\mathcal{F})$. We denote by $Frob_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ a geometric Frobenius at p. We have the following well known result.

THEOREM 11. *The following are true:*

(1) We have that

$$Trace(Frob_p|W) = -\sum_{t \in X(\Gamma_j)(\mathbb{F}_p)} Trace(Frob_p|(i_*\mathcal{F})_t).$$

(2) If the fiber $E_t^j := h_j^{-1}(t)$ is smooth, then

$$Trace(Frob_p|(i_*\mathcal{F})_t) = Trace(Frob_p|H^1(E_t^j, \mathbb{Q}_\ell)) = p + 1 - \#E_t^j(\mathbb{F}_p).$$

Furthermore,

$$Trace(Frob_p|(i_*\mathrm{Sym}^2\mathcal{F})_t) = Trace(Frob_p|(i_*\mathcal{F})_t)^2 - p,$$

and

$$Trace(Frob_p|(i_*\mathrm{Sym}^3\mathcal{F})_t) = Trace(Frob_p|(i_*\mathcal{F})_t)^3 - 2p \cdot Trace(Frob_p|(i_*\mathcal{F})_t).$$

(3) If the fiber E_t^j is singular, then

$$Trace(Frob_p|(i_*\mathcal{F})_t) = \begin{cases} 1 & \text{if the fiber is split multiplicative,} \\ -1 & \text{if the fiber is nonsplit multiplicative,} \\ 0 & \text{if the fiber is additive.} \end{cases}$$

Furthermore, $Trace(Frob_p|(i_*Sym^2\mathcal{F})_t) = 1$ if the fiber is multiplicative or potentially multiplicative (e.g. fiber E_∞^1), and

$$Trace(Frob_p|(i_*Sym^3\mathcal{F})_t) = \begin{cases} 1 & \text{if the fiber is split multiplicative,} \\ -1 & \text{if the fiber is nonsplit multiplicative,} \\ 0 & \text{if the fiber is potentially multiplicative.} \end{cases}$$

Proof. (1) is the consequence of the Lefschetz fixed point formula ([Del77], Rapport 3.2).

For good t, $(i_*\mathcal{F})_t = H^1(E_t^j, \mathbb{Q}_\ell)$, hence the first formula in (2) follows. Note that if λ_1 and λ_2 are eigenvalues of $Frob_p$ acting on $(i_*\mathcal{F})_t$, then $\lambda_1^k, \lambda_1^{k-1}\lambda_2, \ldots, \lambda_1\lambda_2^{k-1}, \lambda_2^k$ are the eigenvalues of $Sym^k Frob_p$ acting on $Sym^k(i_*\mathcal{F})_t$. Since $(i_*Sym^k\mathcal{F})_t = Sym^k(i_*\mathcal{F})_t$, the second part of (2) follows (note that determinant of $Frob_p$ is equal to p).

In order to calculate trace of $Frob_p$ at bad fibers, we follow 3.7 of [Sch88]. If $t \in X(\Gamma_j)(\mathbb{F}_p)$, let K be the function field of the connected component of $X(\Gamma_j) \otimes \mathbb{F}_p$ containing t. Let v be the discrete valuation of K corresponding to t, and K_v the completion. Let G_v be the absolute

Galois group $\mathrm{Gal}(K_v^{\mathrm{sep}}/K_v)$, I_v the inertia group, and F_v a geometric Frobenius. Write $H_v = H^1(E^j \otimes K_v^{\mathrm{sep}}, \mathbb{Q}_\ell)$. Then H_v is a G_v-module and

$$Trace(Frob_p|(i_*\mathrm{Sym}^k\mathcal{F})_t) = Trace(F_v|(Sym^k H_v)^{I_v}).$$

In the case of multiplicative reduction $H_v^{I_v}$ is one dimensional and F_v acts on it as 1 if the reduction is split multiplicative, and as -1 if the reduction is nonsplit multiplicative. If the reduction is additive, then $H_v^{I_v} = \{0\}$. The first formula in (3) follows (see Section 10 of Chapter IV in [Sil94]).

In our situation (see Lemma 5.2 and Exercises 5.11, 5.13 in [Sil94]), inertia subgroup I_v acts on H_v as $\left(\begin{smallmatrix}\chi & * \\ 0 & \chi\end{smallmatrix}\right)$, where $*$ is not identically zero, and χ is the character associated to $L_v = K_v\left(\sqrt{\frac{-c_4(E^j\otimes K_v)}{c_6(E^j\otimes K_v)}}\right)/K_v$. If reduction at v is multiplicative this character is unramified (or trivial), and if the reduction is additive it is ramified. Denote by Y a generator of $H_v^{I(K_v^{sep}/L_v)}$. Then a direct computation shows that Y^2 and Y^3 generate $(Sym^2 H_v)^{I(K_v^{sep}/L_v)}$ and $(Sym^3 H_v)^{I(K_v^{sep}/L_v)}$ respectively. If the reduction is multiplicative, then $I_v = I(K_v^{sep}/L_v)$. If the reduction is potentially multiplicative then I_v acts on Y as ± 1. Hence $(Sym^3 H_v)^{I_v} = \{0\}$, and $(Sym^2 H_v)^{I_v}$ is generated by Y^2. The claim follows.

□

5. Results

To further simplify formulas for $\sum_{t\neq 0,1} W(t)$, we use the following proposition.

Proposition 12. *Let p be an odd prime.*

a) *If $p \equiv 1 \pmod 4$ then*

$$12(\#S_2'' + 2\#S_3'') = 3(p + 1 - c(2,8)).$$

b) *If $p \equiv 3 \pmod 4$ then*

$$\#S_2'' = \frac{1}{8}(p + 1 - c(2,8)) \text{ and } \#S_1' - \#S_1'' = \#S_3.$$

Moreover,

$$\sum_{t\in S_1'} Q(t) = \frac{1}{2}\sum_{t\in T_1} Q(t).$$

Proof. Consider the map

$$g : X(2,8) \to X_1(4), \qquad (E,T,P) \mapsto (E/\langle T\rangle, 2P + \langle T\rangle), \qquad t_1 = \left(\frac{t_4^2-1}{2t_4}\right)^4,$$

where T and P denote points on E of order two and eight respectively, and $E/\langle T\rangle$ is elliptic curve two-isogenous to E with the kernel of isogeny equal to the subgroup generated by T.

This map is not Galois, but, if $p \equiv 1 \pmod 4$ then it has the property that the number of preimages of $t_1 \in X_1(4)(\mathbb{F}_p)$ under g is zero unless $t_1 \in S_2'' \cup S_3''$. To see this, let $(E,T,P) \in X(2,8)(\mathbb{F}_p)$ and identify $(E/\langle T\rangle, 2P+\langle T\rangle)$ with (E_{t_1}, R). In the notation of Section 2, an isogeny $E \to E/\langle T\rangle$ can be identified with ϕ, and by definition $\phi(P) = P + \langle T\rangle$ is a point of order 8 on E_{t_1} that is an element of Γ_{t_1}. Hence $t_1 \in S_2'' \cup S_3''$.

Furthermore, the number of preimages is equal to four if $t_1 \in S_2''$ (since $2P+\langle T\rangle = 2(P+W)+\langle T\rangle$ for all $W \in E(\mathbb{F}_p)[2]$) and eight if $t_1 \in S_3''$. In the second case, there is an additional point

$S \in E(\mathbb{F}_p)$ such that $2S = T$ (S is $\mathbb{F}_p$-rational since in this case $E_{t_1}(\mathbb{F}_p)[2] \subset \Gamma_t = \phi(E(\mathbb{F}_p))$), hence we have that $2P + \langle T\rangle = 2(P+S) + \langle T\rangle$, and the claim follows.

Now we have

$$4\#S_2'' + 8\#S_3'' = \#\left(X(2,8)(\mathbb{F}_p) \setminus cusps\right) = p + 1 - c(2,8),$$

and the claim of part a) follows.

Next, assume that $p \equiv 3 \pmod 4$. Using universality of the family E^1, we can identify affine points (E,R) on $X_1(4)(\mathbb{F}_p)$ with the points $(E_t, R_t = [t,2t])$ for $t \in \mathbb{F}_p \setminus \{0,1\}$. Under this identification, subgroup $\Gamma_t < E_t(\mathbb{F}_p)$ corresponds to the index 2 subgroup of $E(\mathbb{F}_p)$ that contains only one point of order 2 - point $2R$.

Define a map $S_1' \to S_1'' \cup S_3$, by the rule $(E,R) \mapsto (E, R+T)$ for any $T \in E(\mathbb{F}_p)[2] \setminus \{2R\}$. Note that the map is well defined since in $X_1(4)$ we identify $(E, T+R)$ with $(E, -(T+R)) = (E, T+3R)$ and also since $T \notin \Gamma_t$ implies $R + T \in \Gamma_t$. Map is clearly a bijection - its inverse is a map $S_1'' \cup S_3 \to S_1'$ defined by the same rule, thus $\#S_1' - \#S_1'' = \#S_3$. As the map is not changing the elliptic curve, it follows that

$$\sum_{t \in S_1'} Q(t) = \sum_{t \in S_1'' \cup S_3} Q(t),$$

hence

$$\sum_{t \in S_1'} Q(t) = \frac{1}{2} \sum_{t \in T_1} Q(t).$$

Since $p \equiv 3 \pmod 4$, we have that $\sqrt{-1} \notin \mathbb{F}_p$ so it follows from the properties of Weil pairing that elliptic curves over $\mathbb{F}_p$ can not have full 4-torsion. In particular, the number of preimages of $t_1 \in S_2'' \cup S_3$ under the map g is always equal to 4, so

$$4\#S_2'' + 4\#S_3 = \#\left(X(2,8)(\mathbb{F}_p) \setminus cusps\right) = p + 1 - c(2,8).$$

The claim now follows from the fact that

$$\#S_3 = \frac{1}{8}\#\left(X(2,8)(\mathbb{F}_p) \setminus cusps\right) = \frac{1}{8}(p + 1 - c(2,8)),$$

since one $t \in S_3 = T_3$ corresponds to the eight elements in $X(2,8)(\mathbb{F}_p)$ (we can choose a point of order 2 in two ways, and a point of order 8 in four ways). □

It follows from the previous proposition that if $p \equiv 1 \pmod 4$ we have that

$$\begin{aligned} 4! \sum_{t \neq 0,1} W(t) = &\sum_{t \neq 0,1} (Q(t)^3 - 9Q(t)^2 + 23Q(t) - 15) + \sum_{t \in T_1} (3Q(t)^2 - 15Q(t) + 15) \\ &+ \sum_{t \in T_2} (9Q(t) - 21) - \sum_{t \in T_3} (3Q(t) - 21) - 3(p + 1 - c(2,8)), \end{aligned} \tag{2}$$

while for $p \equiv 3 \pmod 4$ we have

$$\begin{aligned} 4! \sum_{t \neq 0,1} W(t) = &\sum_{t \neq 0,1} (Q(t)^3 - 9Q(t)^2 + 23Q(t) - 15) + \sum_{t \in T_1} (3Q(t)^2 - 9Q(t) + 3) \\ &+ \sum_{t \in T_2} (9Q(t) - 21) - \sum_{t \in T_3} (3Q(t) + 3) - \frac{3}{2}(p + 1 - c(2,8)). \end{aligned} \tag{3}$$

Our next goal is to calculate sums of the form $\sum_{t \in T_i} Q(t)^j$. The main observation is that

$T_i = g_{i+1}(X_i(\mathbb{F}_p) - cusps)$, where X_i is equal to the modular curves $X(2,8)$, $X_1(8)$ and $X(2,4)$ for $i = 1, 2, 3$ respectively. Thus, we can replace a summation $\sum_{t \in T_i} Q(t)^j$ with the

$$\sum_{t_{i+1} \in X_i(\mathbb{F}_p) - cusps} \frac{1}{N(t_{i+1})} Q(g_{i+1}(t_{i+1}))^j$$

where $N(t_{i+1}) = \#(g_{i+1}^{-1}(g_{i+1}(t_{i+1})) \cap X_i(\mathbb{F}_p))$ is the number of $\mathbb{F}_p$-rational preimages of $g_{i+1}(t_{i+1})$ under the map g_{i+1}. Maps g_2 and g_4 are Galois, hence in those two cases $N = 2$ and $N = 8$ respectively while for g_3 we have that $N(t) = 4$ if $t \in T_3$ and $N(t) = 2$ if $t \in T_2 \setminus T_3$ (this is because its Galois closure g_4 is generically dihedral of order 8).

5.1 $X_1(4)$

The universal elliptic curve E^1 over $X_1(4)$ has three singular fibers (over the cusps): additive $t = \infty$, split multiplicative $t = 0$, and fiber $t = 1$ which is split multiplicative if $p \equiv 1 \pmod 4$ and nonsplit multiplicative if $p \equiv 3 \pmod 4$. Moreover, the additive fiber $t = \infty$ becomes (split) multiplicative over quadratic extension of the base field.

Proposition 13. *a)*

$$\sum_{t \neq 0,1} P(t) = \begin{cases} p^2 - p \text{ if } p \equiv 1 \pmod 4, \\ p^2 - p - 2 \text{ if } p \equiv 3 \pmod 4. \end{cases}$$

b)

$$\sum_{t \neq 0,1} P(t)^2 = \begin{cases} p^3 + p^2 - p - 1, \text{ if } p \equiv 1 \pmod 4, \\ p^3 + p^2 - 5p - 5, \text{ if } p \equiv 3 \pmod 4. \end{cases}$$

c)

$$\sum_{t \neq 0,1} P(t)^3 = \begin{cases} p^4 + 4p^3 - 4p - 3 + e(p), \text{ if } p \equiv 1 \pmod 4, \\ p^4 + 4p^3 - 6p^2 - 20p - 11 + e(p), \text{ if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. Denote by $\mathcal{F} = R^1 h'_{1*} \mathbb{Q}_\ell$.

a) Parts (1) and (2) of Theorem 11 imply that

$$\begin{aligned} Trace(Frob_p | W^1_{1,\ell}) &= - \sum_{t \in \text{cusps}} Trace(Frob_p | (i_* \mathcal{F})_t) - \sum_{t \neq 0,1} (p + 1 - P(t)), \\ &= \sum_{t \neq 0,1} P(t) - (p^2 - p - 2) - \sum_{t \in \text{cusps}} Trace(Frob_p | (i_* \mathcal{F})_t). \end{aligned}$$

Since $\dim(S_3(\Gamma_1(4))) = 0$ it follows that $Trace(Frob_p | W^1_{1,\ell}) = 0$. Claim now follows from Theorem 11 (3) and the description of reduction types of singular fibers for $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$.

b) Since by Theorem 11(3) the trace at every singular fiber is 1, we have that

$$\begin{aligned} Trace(Frob_p | W^1_{2,\ell}) &= - \sum_{t \in \text{cusps}} Trace(Frob_p | (i_* \text{Sym}^2 \mathcal{F})_t) - \sum_{t \neq 0,1} \Big((p + 1 - P(t))^2 - p \Big), \\ &= -3 - \sum_{t \neq 0,1} P(t)^2 - p^3 + p^2 + p + 2 + 2(p+1) \sum_{t \neq 0,1} P(t). \end{aligned}$$

The claim follows from the part a) since $\dim(S_4(\Gamma_1(4))) = 0$ (hence $Trace(Frob_p|W^1_{2,\ell}) = 0$).
c) Theorem 11 implies that

$$\begin{aligned} Trace(Frob_p|W^1_{3,\ell}) &= -\sum_{t\in\text{cusps}} Trace(Frob_p|(i_*\text{Sym}^3\mathcal{F})_t) - \sum_{t\neq 0,1}\Big((p+1-P(t))^3 - 2p(p+1-P(t))\Big), \\ &= \sum_{t\neq 0,1} P(t)^3 - 3(p+1)\sum_{t\neq 0,1} P(t)^2 + (3(p+1)^2-2p)\sum_{t\neq 0,1} P(t) \\ &- (p-2)(p+1)^3 + 2p(p-2)(p+1) - \sum_{t\in\text{cusps}} Trace(Frob_p|(i_*\text{Sym}^3\mathcal{F})_t). \end{aligned}$$

The claim follows from the parts a) and b) and Proposition 8a) (hence $Trace(Frob_p|W^1_{3,\ell}) = e(p)$). Note that

$$\sum_{t\in\text{cusps}} Trace(Frob_p|(i_*\text{Sym}^3\mathcal{F})_t) = \begin{cases} 0+1+1=2, \text{ if } p\equiv 1 \pmod 4, \\ 0+1+(-1)=0, \text{ if } p\equiv 3 \pmod 4. \end{cases}$$

□

5.2 $X(2,8)$

Universal elliptic curve E^4 over $X(2,8)$ has 10 singular fibers: $t_4 = \pm i$ (two cusps above $t_1 = \infty$) and $t_4^2+2t_4-1=0$ and $t_4^2-2t_4-1=0$ (four cusps above $t_1=1$) which are split multiplicative if $p\equiv 1 \pmod 4$ and nonsplit multiplicative otherwise, and split multiplicative $t_4 = \pm 1, 0, \infty$(four cusps above $t_1 = 0$).

PROPOSITION 14. *a)*

$$\sum_{t\in T_3} 1 = \begin{cases} \frac{p-9}{8}, \text{ if } p\equiv 1 \pmod 8, \\ \frac{p-3}{8}, \text{ if } p\equiv 3 \pmod 8, \\ \frac{p-5}{8}, \text{ if } p\equiv 5 \pmod 8, \\ \frac{p-7}{8}, \text{ if } p\equiv 7 \pmod 8. \end{cases}$$

b)

$$\sum_{t\in T_3} P(t) = \begin{cases} \frac{p^2-8p+1+2b(p)+c(p)}{8}, \text{ if } p\equiv 1 \pmod 8, \\ \frac{p^2-2p+1+2b(p)+c(p)}{8}, \text{ if } p\equiv 3 \pmod 8, \\ \frac{p^2-4p+1+2b(p)+c(p)}{8}, \text{ if } p\equiv 5 \pmod 8, \\ \frac{p^2-6p-7+2b(p)+c(p)}{8}, \text{ if } p\equiv 7 \pmod 8. \end{cases}$$

Proof. a) Since T_3 is equal to the image of $\mathbb{F}_p$-points (which are not cusps) on $X(2,8)$ under the natural map $g_4 : X(2,8) \to X_1(4)$ of degree 8, we have $\sum_{t\in T_3} 1 = \frac{p+1-c(2,8)}{8}$, since $\#X(2,8)(\mathbb{F}_p) = p+1$ and g_4 is Galois. The claim follows.
b) From the definition of T_3 we have

$$\sum_{t\in T_3} P(t) = \frac{1}{8}\sum_{t_4\in X(2,8)(\mathbb{F}_p)\setminus cusps} P(g_4(t_4)).$$

Denote $\mathcal{F} = R^1 h'_{4*}\mathbb{Q}_\ell$. Theorem 11 implies that (the sum is over $X(2,8)(\mathbb{F}_p)$)

$$\begin{aligned} Trace(Frob_p|W_{1,\ell}^4) &= -\sum_{t\in\text{cusps}} Trace(Frob_p|(i_*\mathcal{F})_t) - \sum_{t\notin\text{cusps}} (p+1-P(g_4(t)))\,, \\ &= -\sum_{t\in\text{cusps}} Trace(Frob_p|(i_*\mathcal{F})_t) - (p+1)(p+1-c(2,8)) + \sum_{t\notin\text{cusps}} P(g_4(t)). \end{aligned}$$

It follows from Proposition 8b) that $Trace(Frob_p|W_{1,\ell}^4) = 2b(p) + c(p)$. The claim follows since Theorem 11(3) implies

$$\sum_{t\in\text{cusps}} Trace(Frob_p|(i_*\mathcal{F})_t) = \begin{cases} 10, & \text{if } p\equiv 1 \pmod 8, \\ 4, & \text{if } p\equiv 3 \pmod 8, \\ 6, & \text{if } p\equiv 5 \pmod 8, \\ 0, & \text{if } p\equiv 7 \pmod 8. \end{cases}$$

□

5.3 $X_1(8)$

Universal elliptic curve E^3 over $X_1(8)$ has 6 singular fibers: split multiplicative $t_3 = \infty$ and $t_3 = \pm 1$ (two cusps above $t_1 = 0$) and $t_3 = 0, \pm\sqrt{2}$ (three cusps above $t_1 = 1$) which are split multiplicative if $p \equiv 1 \pmod 4$ and nonsplit multiplicative otherwise. Denote $\mathcal{F} = R^1 h'_{3*}\mathbb{Q}_\ell$.

Proposition 15. *a)*

$$\sum_{t\in T_2} 1 = \begin{cases} \frac{3p-11}{8}, & \text{if } p\equiv 1 \pmod 8, \\ \frac{3p-9}{8}, & \text{if } p\equiv 3 \pmod 8, \\ \frac{3p-7}{8}, & \text{if } p\equiv 5 \pmod 8, \\ \frac{3p-13}{8}, & \text{if } p\equiv 7 \pmod 8. \end{cases}$$

b)

$$\sum_{t\in T_2} P(t) = \begin{cases} \frac{3p^2-8p+2b(p)-c(p)+3}{8}, & \text{if } p\equiv 1 \pmod 8, \\ \frac{3p^2-6p+2b(p)-c(p)-5}{8}, & \text{if } p\equiv 3 \pmod 8, \\ \frac{3p^2-4p+2b(p)-c(p)+3}{8}, & \text{if } p\equiv 5 \pmod 8, \\ \frac{3p^2-10p+2b(p)-c(p)-13}{8}, & \text{if } p\equiv 7 \pmod 8. \end{cases}$$

Proof. a) By definition, T_2 is equal to the image of $\mathbb{F}_p$-points (which are not cusps) on $X_1(8)$ under the natural map $g_3 : X_1(8) \to X_1(4)$ of degree 4. Since we have $p+1-c(8) = 4\sum_{t\in T_3} 1 + 2\sum_{t\in T_2} 1$, the claim follows.
b) From the discussion at a beginning of this section it follows that

$$4\sum_{t\in T_3} P(t) + 2\sum_{t\in T_2\setminus T_3} P(t) = \sum_{t_3\in X_1(8)(\mathbb{F}_p)\setminus cusps} P(g_3(t_3)),$$

hence

$$\sum_{t\in T_2} P(t) = \frac{1}{2}\sum_{t_3\in X_1(8)(\mathbb{F}_p)\setminus cusps} P(g_3(t_3)) - \sum_{t\in T_3} P(t).$$

Denote $\mathcal{F} = R^1h'_{3*}\mathbb{Q}_\ell$. Theorem 11 implies that

$$\begin{aligned} Trace(Frob_p|W^3_{1,\ell}) &= -\sum_{t\in\text{cusps}} Trace(Frob_p|(i_*\mathcal{F})_t) - \sum_{t\notin\text{cusps}} (p+1-P(g_3(t)))\,, \\ &= -\sum_{t\in\text{cusps}} Trace(Frob_p|(i_*\mathcal{F})_t) - (p+1)(p+1-c(8)) + \sum_{t\notin\text{cusps}} P(g_3(t)), \end{aligned}$$

where the sums are over $X_1(8)(\mathbb{F}_p)$. It follows from Proposition 8c) that $Tr(Frob_p|W^3_{1,\ell}) = b(p)$, and the claim follows. Note that Theorem 11 implies

$$\sum_{t\in\text{cusps}} Tr(Frob_p|(i_*\mathcal{F})_t) = \begin{cases} 6, \text{ if } p\equiv 1 \pmod 8, \\ 2, \text{ if } p\equiv 3 \pmod 8, \\ 4, \text{ if } p\equiv 5 \pmod 8, \\ 0, \text{ if } p\equiv 7 \pmod 8. \end{cases}$$

□

5.4 $X(2,4)$

Universal elliptic curve E^2 over $X(2,4)$ has 4 singular fibers: $t_2 = 0$ (the cusp above $t_1 = 1$) and $t_2 = \infty$ which are split multiplicative if $p \equiv 1 \pmod 4$ and nonsplit multiplicative otherwise, and split multiplicative $t_2 = \pm 1$ (two cusps above $t_1 = 0$).

PROPOSITION 16. *a)*

$$\sum_{t\in T_1} 1 = \frac{p-3}{2},$$

b)

$$\sum_{t\in T_1} P(t) = \begin{cases} \frac{(p-1)^2}{2}, \text{ if } p\equiv 1 \pmod 4, \\ \frac{p^2-2p-3}{2}, \text{ if } p\equiv 3 \pmod 4. \end{cases}$$

c)

$$\sum_{t\in T_1} P(t)^2 = \begin{cases} \frac{p^3+1-d(p)}{2}, \text{ if } p\equiv 1 \pmod 4, \\ \frac{p^3-8p-7-d(p)}{2}, \text{ if } p\equiv 3 \pmod 4 \end{cases}$$

Proof. Denote $\mathcal{F} = R^1h'_{2*}\mathbb{Q}_\ell$.

a) By definition, T_1 is equal to the image of $\mathbb{F}_p$-points (which are not cusps) on $X(2,4)$ under the natural map $g_2 : X(2,4) \to X_1(4)$ of degree 2. Since g_2 is Galois, we have $p+1-c(2,4) = 2\sum_{t\in T_1} 1$ and the claim follows.

b) It follows from the discussion at the beginning of this section that

$$\sum_{t\in T_1} P(t) = \frac{1}{2} \sum_{t_2\in X(2,4)(\mathbb{F}_p)\setminus cusps} P(g_2(t_2)).$$

Theorem 11 implies

$$\begin{aligned} Trace(Frob_p|W^2_{1,\ell}) &= -\sum_{t\in\text{cusps}} Trace(Frob_p|(i_*\mathcal{F})_t) - \sum_{t\notin\text{cusps}} (p+1-P(g_2(t)))\,, \\ &= -\sum_{t\in\text{cusps}} Trace(Frob_p|(i_*\mathcal{F})_t) - (p+1)(p+1-c(2,4)) + \sum_{t\notin\text{cusps}} P(g_2(t)), \end{aligned}$$

where the sums are over $X(2,4)(\mathbb{F}_p)$. Since $\dim S_3(\Gamma_1(4)\cap\Gamma^0(2))=0$, it follows $Trace(Frob_p|W_{1,\ell}^2)=0$, and the claim follows. Note that we used

$$\sum_{t\in\text{cusps}} Trace(Frob_p|(i_*\mathcal{F})_t)=\begin{cases}4, & \text{if } p\equiv 1 \pmod 4,\\ 0, & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

c) We have $\sum_{t\in T_1} P(t)^2=\frac{1}{2}\sum_{t_2\in X(2,4)(\mathbb{F}_p)\setminus cusps} P(g_2(t_2))^2$. Theorem 11 implies

$$\begin{aligned}Trace(Frob_p|W_{2,\ell}^2) &= -\sum_{t\in\text{cusps}} Trace(Frob_p|(i_*\text{Sym}^2\mathcal{F})_t)-\sum_{t\notin\text{cusps}}\Big((p+1-P(g_2(t)))^2-p\Big),\\ &= -\sum_{t\notin\text{cusps}} P(g_2(t))^2+2(p+1)\sum_{t\notin\text{cusps}} P(g_2(t))-(p+1-c(2,4))(p^2+p+1)\\ &\quad -\sum_{t\in\text{cusps}} Trace(Frob_p|(i_*\text{Sym}^2\mathcal{F})_t),\end{aligned}$$

where the sums are over $X(2,4)(\mathbb{F}_p)$.

It follows from Proposition 8d) that $Trace(Frob_p|W_{2,\ell}^2)=d(p)$. The claim follows. Note that we used

$$\sum_{t\in\text{cusps}} Trace(Frob_p|(i_*\text{Sym}^2\mathcal{F})_t)=4.$$

□

5.5 Proof of Theorem 1

The claim follows from the formula

$$N^{(4)}(p)=\sum_{t\in\mathbb{F}_p\setminus\{0\}} W(t)=W(1)+\sum_{t\neq 0,1} W(t),$$

by substituting results from Propositions 13-16 into formulas (2) and (3) and from Proposition 7 which provides formula for $W(1)$.

6. Diophantine m-tuples in $\mathbb{F}_p$ and character sums

In this section, we will use properties of character sums (sums of the Legendre symbols) to show that for arbitrary $m\geqslant 2$ there exist Diophantine m-tuples in $\mathbb{F}_p$ for sufficiently large p. We will also derive formulas for the number of Diophantine pairs and triples in $\mathbb{F}_p$.

Theorem 17. *Let $m\geqslant 2$ be an integer. If $p>2^{2m-2}m^2$ is a prime, then there exists a Diophantine m-tuple in $\mathbb{F}_p$.*

Proof. We prove the theorem by induction on m. For $m=2$ and $p>16$ (in fact, for $p\geqslant 5$), we may take the Diophantine pair $\{1,3\}$ in $\mathbb{F}_p$.

Let $m\geqslant 2$ be an integer such that the statement holds. Take a prime $p>2^{2m}(m+1)^2$. Since $p>2^{2m-2}m^2$, there exists a Diophantine m-tuple $\{a_1,\ldots,a_m\}$ in $\mathbb{F}_p$. Let

$$g:=\#\{x\in\mathbb{F}_p\,:\,\left(\frac{a_ix+1}{p}\right)=1,\text{ for } i=1,\ldots,m\}$$

and denote by $\bar{a}_i$ the multiplicative inverse of a_i in $\mathbb{F}_p$. Then, by [LN97, Exercise 5.64], we have

$$\begin{aligned} g=&\#\{x \in \mathbb{F}_p : \left(\frac{x+\bar{a}_i}{p}\right) = \left(\frac{\bar{a}_i}{p}\right), \text{ for } i = 1, \dots, m\} \\ \geqslant&\frac{p}{2^m} - \left(\frac{m-2}{2} + \frac{1}{2^m}\right)\sqrt{p} - \frac{m}{2}. \end{aligned}$$

Since,

$$\begin{aligned} \left(\frac{m-2}{2} + \frac{1}{2^m}\right)\sqrt{p} + \frac{m}{2} + (m+1) &< \left(\frac{m-2}{2} + \frac{1}{2^m}\right)\sqrt{p} + \frac{3}{2}(m+1) \\ &< \sqrt{p}\left(\frac{m}{2} - 1 + \frac{1}{2^m} + \frac{3}{2^{m+1}}\right) < \frac{m}{2}\sqrt{p} < \frac{p}{2^{m+1}} < \frac{p}{2^m}, \end{aligned}$$

we get that $g > m+1$. Thus, we conclude that there exist $x \in \mathbb{F}_p$, $x \notin \{0, a_1, a_2, \dots, a_m\}$, such that $\left(\frac{a_i x+1}{p}\right) = 1$ for $i = 1, \dots, m$. Hence, $\{a_1, \dots, a_m, x\}$ is a Diophantine $(m+1)$-tuple in $\mathbb{F}_p$. □

REMARK 1. *Using the Weil bounds for curves we can get a slightly better lower bound for g. Let $a_1, a_2, \dots, a_m$ be distinct elements of $\mathbb{F}_p^\times$. A desingularisation T_m of a projective curve defined by the equations $a_i xz + z^2 = t_i^2$ for $i = 1, 2, \dots m$ has genus $g_m = (m-3)2^{m-2} + 1$ (to see this apply Riemann-Hurwitz formula to the natural projection $T_m \to T_{m-1}$). Hence the Weil bound for T_m implies that $\#T_m(\mathbb{F}_p) \geqslant p + 1 - 2g_m\sqrt{p}$. We can write $\#T_m(\mathbb{F}_p) = 2^{m-1} + 2^m g + 2^{m-1}N$ where $2^{m-1}N$ is the number of points on T_m with one coordinate t_i equal to zero and 2^{m-1} is the number of points at infinity. From $N \leqslant m$ it follows that $g \geqslant \frac{p+1}{2^m} - \left(\frac{m-3}{2} + \frac{1}{2^{m-1}}\right)\sqrt{p} - \frac{m+1}{2}$.*

In the proof of the next two propositions we will several times use the following well-known fact (see e.g. [Hua82, Section 7.8]):

$$\sum_{x \in \mathbb{F}_p} \left(\frac{\alpha x^2 + \beta x + \gamma}{p}\right) = -\left(\frac{\alpha}{p}\right), \tag{4}$$

provided $\beta^2 - 4\alpha\gamma \not\equiv 0 \pmod{p}$.

PROPOSITION 18. *Let p be an odd prime. The number of Diophantine pairs in $\mathbb{F}_p$ is equal to*

$$N^{(2)}(p) = \begin{cases} \frac{(p-1)(p-2)}{4}, & \text{if } p \equiv 1 \pmod 4, \\ \frac{p^2-3p+4}{4}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. We have

$$4N^{(2)}(p) = \sum_{a,b \neq 0, a \neq b} \left(1 + \left(\frac{ab+1}{p}\right)'\right),$$

where $\left(\frac{x}{p}\right)' = \left(\frac{x}{p}\right)$ for $x \neq 0$ and $\left(\frac{0}{p}\right)' = 1$. Therefore, we have

$$\begin{aligned} 4N^{(2)}(p) &= \sum_{b \neq 0} \sum_{a \neq 0, b} 1 + \sum_{b \neq 0} \sum_{a \neq 0, b} \left(\frac{ab+1}{p}\right) + \sum_{b \neq 0, b^2 \neq -1} 1 \\ &= (p-1)(p-2) + \sum_{b \neq 0} \left(-1 - \left(\frac{b^2+1}{p}\right)\right) + \sum_{b \neq 0, b^2 \neq -1} 1. \end{aligned}$$

If $p \equiv 1 \pmod 4$, the last sum is equal to $p-3$. Thus we get

$$4N^{(2)}(p) = (p-1)(p-2) - (p-1) + 2 + (p-3) = (p-1)(p-2).$$

Similarly, for $p \equiv 3 \pmod 4$, we get

$$4N^{(2)}(p) = (p-1)(p-2) - (p-1) + 2 + (p-1) = p^2 - 3p + 4.$$

□

There is a birational map $V_3 \to V_3'$, where V_3' is the affine hypersurface given by $(x^2-1)(y^2-1) = z^2 - w^2$, sending $(a_1, a_2, a_3, t_{12}, t_{13}, t_{23})$ to $(x, y, z, w) = (t_{12}, t_{13}, a_1 t_{23}, a_1)$. Note that this is an isomorphism on U_3 (the inverse is defined if and only if $z^2 - w^2 \neq 0$). Define V_3'' to be the open subset of V_3' where $z^2 \neq w^2$, i.e. V_3'' is the image of elements in V_3 for which $a_1 a_2 a_3 \neq 0$.

Proposition 19. *Let p be an odd prime. Then*

$$\#V_3''(\mathbb{F}_p) = p^3 - 5p^2 + 8p - 4.$$

Proof. Since the formula (4) for $k \in \mathbb{F}_p^\times$ implies

$$\#\{(z,w) \in \mathbb{F}_p^2 | z^2 - w^2 = k\} = \sum_{w \in \mathbb{F}_p} \left(\left(\frac{w^2 + k}{p} \right) + 1 \right) = p - 1,$$

it follows from Proposition 13a)

$$\begin{aligned}
\#V_3''(\mathbb{F}_p) &= (p-1) \sum_{k \in \mathbb{F}_p^\times} \#\mathcal{D}_k(\mathbb{F}_p) = (p-1) \left(\sum_{k \in \mathbb{F}_p^\times - \{1\}} (\#E_k(\mathbb{F}_p) - 4) + (p-3) - \left(\frac{-1}{p} \right) \right) \\
&= (p-1) \left(\sum_{k \in \mathbb{F}_p^\times - \{1\}} (P(k) - 4) + (p-3) - \left(\frac{-1}{p} \right) \right) \\
&= p^3 - 6p^2 + 9p - 3 - \left(\frac{-1}{p} \right) + \sum_{k \in \mathbb{F}_p^\times - \{1\}} P(k) = p^3 - 5p^2 + 8p - 4,
\end{aligned}$$

where $\mathcal{D}_k$ and E_k are defined in Section 2 and $P(k) = \#E_k(\mathbb{F}_p)$. (It is easy to check that for $k \neq 1$, $\#E_k(\mathbb{F}_p) = \#\mathcal{D}_k(\mathbb{F}_p) - 4$ and $\#\mathcal{D}_1(\mathbb{F}_p) = (p-3) - \left(\frac{-1}{p}\right)$.) □

If we remove from $V_3''(\mathbb{F}_p)$ the points that are in the image of the points $(a_1, a_2, a_3, t_{12}, t_{13}, t_{23})$ for which a_i are not pairwise distinct, we obtain the formula for $\#U_3(\mathbb{F}_p)$.

Corollary 20. *Let p be an odd prime. Then*

$$\#U_3(\mathbb{F}_p) = \begin{cases} p^3 - 12p^2 + 53p - 90, & \text{if } p \equiv 1 \pmod 4, \\ p^3 - 12p^2 + 53p - 78, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Finally, we can prove the formula for the number of Diophantine triples $N^{(3)}(p)$ in $\mathbb{F}_p$.

Proposition 21. *Let p be an odd prime. The number of Diophantine triples in $\mathbb{F}_p$ is equal to*

$$N^{(3)}(p) = \begin{cases} \frac{(p-1)(p-3)(p-5)}{48}, & \text{if } p \equiv 1 \pmod 4, \\ \frac{(p-3)(p^2-6p+17)}{48}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. Since the triples corresponding to the elements in $U_3(\mathbb{F}_p)$ are pairwise distinct, the size of a G_3-orbit in $U_3(\mathbb{F}_p)$ is either $8 \cdot 3!$ (if all t_i are non-zero) or $4 \cdot 3!$ (if there is one t_i equal to zero).

The number of the later orbits is equal to the number of Diophantine triples $\{a, b, c\}$ in $\mathbb{F}_p$ for which $ab + 1 = 0$. It is not hard to see that the number of such triples is equal to $\frac{p^2-10p+25}{8}$ if $p \equiv 1 \pmod 4$ and $\frac{p^2-6p+9}{8}$ if $p \equiv 3 \pmod 4$. The number of G_3-orbits of size $8 \cdot 3!$ is then equal to

$$\begin{cases} \frac{\#U_3(\mathbb{F}_p)-3(p^2-10p+25)}{8\cdot 3!}, & \text{if } p \equiv 1 \pmod 4 \\ \frac{\#U_3(\mathbb{F}_p)-3(p^2-6p+9)}{8\cdot 3!}, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

hence the claim follows from Corollary 20.

□

We can now prove the asymptotic formula

$$N^{(m)}(p) = \frac{1}{2^{\binom{m}{2}}} \frac{p^m}{m!} + o(p^m).$$

Since V_m is m-dimensional and geometrically irreducible, it follows that $H_c^{2m}(\overline{V_m}, \mathbb{Q}_\ell)$ is one dimensional and of Tate type of weight $2m$. Hence from the Weil conjectures and the Lefschetz trace formula

$$\#V_m(\mathbb{F}_p) = \sum_{i=0}^{2m} (-1)^i \, Trace\left(Frob_p | H_c^i(\overline{V_m}, \mathbb{Q}_\ell)\right),$$

it follows that $\#V_m(\mathbb{F}_p) = p^m + o(p^m)$. Moreover, since U_m is an open subset of V_m of the maximal dimension, we also have $\#U_m(\mathbb{F}_p) = p^m + o(p^m)$. The size of the generic orbit of G_m acting on $U_m(\mathbb{F}_p)$ is $m! \cdot 2^{\binom{m}{2}}$ (the union of the orbits of smaller size is contained in the union of subvarieties of smaller dimension), hence the asymptotic formula follows.

Acknowledgements

We would like to thank Ivica Gusić, Filip Najman and Anthony Scholl for some helpful comments. This work was supported by the QuantiXLie Centre of Excellence, a project cofinanced by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004). A.D. was supported by the Croatian Science Foundation under the project no. 6422., and both authors were suported by the Croatian Science Foundation under the project no. IP-2018-01-1313.

References

ALL08 A. O. L. Atkin, W.-C. W. Li, L. Long, *On Atkin-Swinnerton-Dyer congruence relations (2)*, Math. Ann. **340** (2008), no. 2, 335–358.

BN16 P. Bruin, F. Najman, *A criterion to rule out torsion groups for elliptic curves over number fields*, Res. Number Theory **2** (2016), no. 3, 1–13.

Del77 P. Deligne, *Cohomologie étale (SGA $4\frac{1}{2}$)*, Lect. Notes in Math. **569** (1977)

Duj97 A. Dujella, *On Diophantine quintuples*, Acta Arith. **81** (1997), 69–79.

Duj04 A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214.

Duj16 A. Dujella, *What is...a Diophantine m-tuple?*, Notices of the AMS **63**, 7 (2016), 772–774.

DujKaz A. Dujella, M. Kazalicki, *More on Diophantine sextuples*, In:Number Theory – Diophantine Problems, Uniform Distribution and Applications, Festschrift in honour of Robert F. Tichy's 60th birthday (C. Elsholtz, P. Grabner, Eds.), Springer-Verlag, Berlin, pp. (2017), 227–235.

DKMS16 A. Dujella, M. Kazalicki, M. Mikić, M. Szikszai, *There are infinitely many rational Diophantine sextuples*, Int. Math. Res. Not. IMRN **2017 (2)** (2017), 490–508.

Gibbs P. E. Gibbs, *A survey of rational Diophantine sextuples of low height*, preprint, 2016.

HTZ B. He, A. Togbé and V. Ziegler, *There is no Diophantine quintuple*, Trans. Amer. Math. Soc. 371 (2019), 6665-6709.

Hua82 L. K. Hua, *Introduction to Number Theory*, Springer-Verlag, (1982).

Kato04 K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Cohomologies p-adiques et applications arithmétiques. III. Astérisque **295** (2004), 117–290.

Iwa97 H. Iwaniec, *Topics in Classical Automorphic Forms*, American Mathematical Society, Providence, RI, (1997).

LMFDB The LMFDB Collaboration, *The L-functions and Modular Forms Database*, http://www.lmfdb.org, (2016)[Online; accessed 20 September 2016].

LN97 R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, (1997).

MS10 R. L. Miller, M. Stoll, *Explicit isogeny descent on elliptic curves*, Math. Comp. **82** (2013), 513–529.

Ono03 K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series*, CBMS Regional Conference Series in Mathematics, **102** (2003).

SAGE *SageMath, the Sage Mathematics Software System (Version 7.2.)*, The Sage Developers, 2016, `http://www.sagemath.org`.

Sch85 A. J. Scholl, *Modular forms and de Rham cohomology; Atkin-Swinnerton-Dyer congruences*, Invent. Math. **79** (1985), 49–77.

Sch88 A. J. Scholl, *The l-adic representations attached to a certain noncongurence subgroup*, J. reine angew. Math. **392** (1988), 1–15.

Sil09 J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Graduate Texts in Mathematics, vol. **106**, Springer, Dordrecht, (2009).

Sil94 J. H. Silverman, *Advanced Topics in the Arithmetics of Elliptic Curves*, Graduate Texts in Mathematics, vol. **151**, Springer-Verlag, New York, (1994).

Andrej Dujella duje@math.hr
Department of Mathematics, Faculty of Science, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia

Matija Kazalicki matija.kazalicki@math.hr
Department of Mathematics, Faculty of Science, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia