The Sato–Tate Conjecture

Nir Elber

Fall 2024

Abstract

This is an expository note for two talks on the Sato–Tate conjecture. In the first talk, we will state the Sato–Tate conjecture for abelian varieties. In the second talk, we will discuss some results related to Sato–Tate groups of the so-called Fermat curves $y^p = x^a(x-1)$, where p is prime and $a \in \{1, 2, \dots, p-1\}$.

Contents

1 Stating the Sato–Tate Conjecture

In this first talk, we will work our way towards stating the Sato–Tate conjecture for abelian varieties. We will gradually increase the amount of assumed background.

1.1 Quadratic Equations

In order to get a dishonest taste for the sort of results we are after, we will begin with the case of quadratic equations. Fix a monic quadratic polynomial $f(x) = x^2 + ax + b$ with nonzero discriminant $a^2 - 4b$, and consider the curve

$$C \colon y^2 = f(x).$$

Technically speaking, we understand C_f to cut out a smooth projective curve in $\mathbb{P}^2_{\mathbb{Q}}$ given by homogenizing.

Example 1. For this section, it will be enough to follow the example $C\colon y^2 = x^2 + 1$ around. The polynomial $x^2 + 1$ has discriminant -4.

Because this is a talk about arithmetic geometry, we are interested in the number of points on C_f. Studying points over $\mathbb{Q}$ or $\mathbb{Z}$ is rather difficult (and will continue to get harder when we change the curve later), so we will content ourselves with studying the number of points over finite fields. Even though our curve is a priori defined over $\mathbb{Q}$, we see that $f(x) \in \mathbb{Z}[x]$ allows us to give C_f a model over $\mathbb{Z}$ given by the same equation. In this way, we can formally make sense of $C(\mathbb{F}_q)$ for any finite field $\mathbb{F}_q$.

Remark 2. In practice, one can think about $C(\mathbb{F}_q)$ as the number of pairs $(x, y) \in \mathbb{F}_q^2$ satisfying the equation given by C. The above process of finding an integral model should be thought of as some formal general procedure.

Remark 3. Our choice of integral model may not always make sense at all primes p. Notably, we would like for C_f to define a smooth curve over $\mathbb{F}_p$, but this requires $a^2 - 4b \neq 0$ (for example). (For odd primes p, smoothness is equivalent to $a^2 - 4b \neq 0$.) Over $\mathbb{Q}$, this was a hypothesis, but in general, $a^2 - 4b$ can vanish $\pmod p$ for some primes p. For example, $y^2 = x^2 + 1$ fails to be smooth over $\mathbb{F}_2$.

Let us begin with an expectation for $C(\mathbb{F}_q)$. For each $x \in \mathbb{F}_q$, it will be difficult to control the value of $f(x)$. However, about half of $\mathbb{F}_q$ has two square roots, and about half of $\mathbb{F}_q$ has no square roots, so it seems reasonably to expect that each $f(x) \in \mathbb{F}_q$ has on average one square root. Thus, we may expect that

$$C(\mathbb{F}_q) \approx q + 1,$$

where we have added 1 to include the point(s) at infinity. Let's see what we get.

Example 4. We continue with the curve $C\colon y^2 = x^2 + 1$. A computer program gives the following output.

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$\#C(\mathbb{F}_p)$	4	6	8	12	14	18	20	24	30	32	38	42	44	48
$p+1$	4	6	8	12	14	18	20	24	30	32	38	42	44	48

Huh, it looks like our guess was pretty spot-on.

Exercise 5. For a curve $C\colon y^2 = x^2 + d$ for some $d \in \mathbb{Z}$, show that $\#C(\mathbb{F}_q) = q + 1$ for any finite field $\mathbb{F}_q$. You may find it helpful to use the substitution $(s, d) = (x + y, x - y)$.

Remark 6. Intuitively, what is going on here is that quadratics cut out genus 0 curves, which must all be isomorphic to $\mathbb{P}^1$.

1.2 Two Elliptic Curves

Let's move on to a more nontrivial example. Most of this first talk will be interested in elliptic curves, for which we pick up the following concrete definition.

Definition 7 (elliptic curve)**.** Fix a field K of characteristic not equal to 2 or 3. Then an *elliptic curve* is a curve of the form

$$E\colon y^2 = x^3 + ax + b,$$

where $a, b \in K$, and the discriminant $-4a^3 - 27b^2$ is nonzero. As usual, E is understood to cut out a smooth projective curve in $\mathbb{P}^2_K$ given by homogeneizing to $Y^2Z = X^3 + aXZ^2 + bZ^3$, so there is one point $[0 : 1 : 0]$ at infinity.

For today, all of our elliptic curves E will be defined over $\mathbb{Q}$ and pretty good integral models.

Example 8. For any lattice $\Lambda \subseteq \mathbb{C}$, it turns out that one can realize $\mathbb{C}/\Lambda$ as an elliptic curve over $\mathbb{C}$.

Example 9. We will follow around the two elliptic curves

$$E_1 \colon y^2 = x^3 + 1 \qquad \text{and} \qquad E_2 \colon y^2 = x^3 + x + 1$$

for this section. Though they look similar, these two curves have very different behavior!

As in the previous section, we note that one can frequently define a notion of $E(\mathbb{F}_q)$. Namely, the cubic equation defining E will only have finitely many denominators, and the discriminant of the cubic equation will only have finitely many prime factors; away from these primes, the equation defining E will define a perfectly reasonable elliptic curve over $\mathbb{F}_{p^r}$ for any $r \geq 1$.

Example 10. We discuss models for our elliptic curves E_1 and E_2. Note that their defining equations have no denominators.

- We see that $E_1 \colon y^2 = x^3 + 1$ has discriminat -27, so we get an elliptic curve over $\mathbb{F}_{p^r}$ for any $p \neq 3$.
- Similarly, the curve $E_2 \colon y^2 = x^3 + x + 1$ has discriminant -31, so we get an elliptic curve over $\mathbb{F}_{p^r}$ for any $p \neq 31$.

Once again, for any value of x, there is no reason to expect $x^3 + ax + b$ to be a square or not, so a reasonable expectation is for

$$E(\mathbb{F}_q) \approx q + 1.$$

Let's see what we get.

Example 11. We continue with the two elliptic curves $E_1 \colon y^2 = x^3 + 1$ and $E_2 \colon y^2 = x^3 + x + 1$.

p	5	7	11	13	17	19	23	29	37	41	43	47
$\#E_1(\mathbb{F}_p)$	6	12	12	12	18	12	24	30	48	42	36	48
$\#E_2(\mathbb{F}_p)$	9	5	14	18	18	21	28	36	48	35	34	60
$p+1$	6	8	12	14	18	20	24	30	38	42	44	48

Our guess seems to be pretty close but not quite spot-on. Let's examine the error.

Example 12. We continue with the two elliptic curves $E_1 \colon y^2 = x^3 + 1$ and $E_2 \colon y^2 = x^3 + x + 1$.

p	5	7	11	13	17	19	23	29	37	41	43	47
$\#E_1(\mathbb{F}_p) - (p+1)$	0	4	0	-2	0	-8	0	0	10	0	-8	0
$\#E_2(\mathbb{F}_p) - (p+1)$	3	-3	2	4	0	1	4	6	10	-7	-10	12

The error seems to be small, but perhaps it is difficult to quantify. We now state a theorem.

Theorem 13 (Hasse–Weil). Fix an elliptic curve E defined over a finite field $\mathbb{F}_q$. Then

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

We will not prove this, but we will state a more general version later. For now, we will content ourselves with the following example.

Example 14. We continue with the two elliptic curves $E_1 \colon y^2 = x^3 + 1$ and $E_2 \colon y^2 = x^3 + x + 1$.

p	5	7	11	13	17	19	23	29	37	41	43	47
$E_1(\mathbb{F}_p) - (p+1)$	0	4	0	−2	0	−8	0	0	10	0	−8	0
$E_2(\mathbb{F}_p) - (p+1)$	3	−3	2	4	0	1	4	6	10	−7	−10	12
$\lfloor 2\sqrt{p} \rfloor$	4	5	6	7	8	8	9	10	12	12	13	13

The bound seems to hold and even come close to equality quite frequently! This motivates us to define

$$a_q(E) := \frac{\#E(\mathbb{F}_q) - (q+1)}{\sqrt{q}} \in [-2, 2].$$

Here is the table again.

Example 15. We continue with the two elliptic curves $E_1 \colon y^2 = x^3 + 1$ and $E_2 \colon y^2 = x^3 + x + 1$.

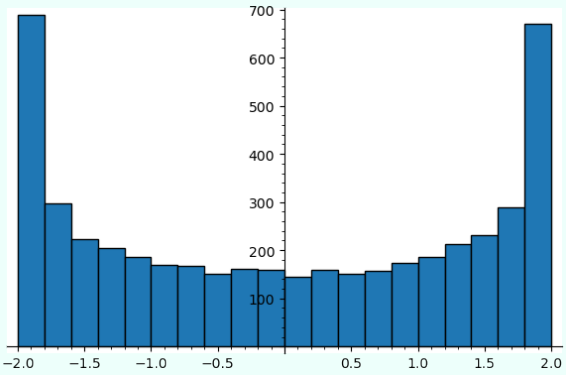
p	5	7	11	13	17	19	23	29	37	41	43	47
$a_p(E_1)$	0.00	1.51	0.00	−0.56	0.00	−1.84	0.00	0.00	1.64	0.00	−1.22	0.00
$a_p(E_2)$	1.34	−1.13	0.60	1.11	0.00	0.23	0.83	1.11	1.64	−1.09	−1.53	1.75

These numbers appear sufficiently random (aside from maybe the large number of 0s), so we can state a heuristic.

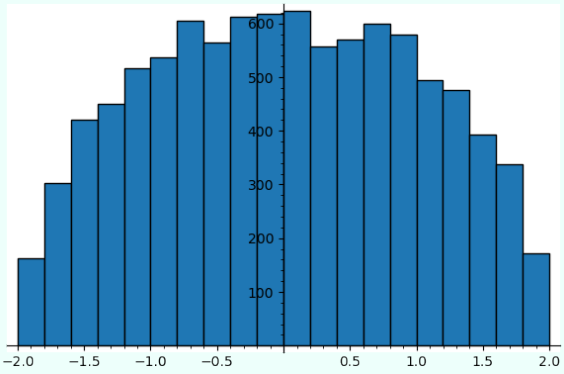
Conjecture 16 (Sato–Tate)**.** Fix an elliptic curve E defined over $\mathbb{Q}$. Then the numbers $a_p(E)$ equidistribute.

This conjecture is correct if we correctly interpret the word "equidistribute." We will spend most of the talk figuring out how to do this. For example, we do not expect the $a_p(E)$s to equidistribute in $[-2, 2]$, as the following examples show.

Example 17. Here is a histogram of the values of $a_p(E_1)$ for $p < 10^5$.



Example 18. Here is a histogram of the values of $a_p(E_2)$ for $p < 10^5$.



These are remarkable histograms! We encourage the reader to investigate other elliptic curves.

Remark 19. It turns out that "most of the time" we will get a semicircle distribution as in Example 18.

A primary goal of the talk is to explain the source of these strange curves.

1.3 The Weil Conjectures

This subsection is included for motivational purposes only and can therefore be skipped without loss of too much continuity.

It will turn out that the values of $a_p(E)$ are controlled by a Galois representation attached to E. The most concrete way to construct this Galois representation is to use the Tate module, which we will do shortly. However, for motivation, we will state the Weil conjectures and explain how they solve our problem.

Theorem 20 (Weil conjectures)**.** Fix a smooth projective variety X over a finite field $\mathbb{F}_q$ of dimension n. Then the formal power series

$$\zeta_X(T) \coloneqq \exp\left(\sum_{r=1}^{\infty} \#X\left(\mathbb{F}_{q^r}\right) \frac{T^r}{r}\right)$$

admits the following desirable properties.

(a) Rationality: one can write

$$\zeta_X(T) = \frac{P_1(T)\cdots P_{2n-1}(T)}{P_2(T)\cdots P_{2n}(T)}$$

for polynomials $P_\bullet(T) \in 1 + T\mathbb{Z}[T]$.

(b) Riemann hypothesis: the roots of the polynomial $P_\bullet(T)$ are complex numbers with roots of magnitude $q^{-\bullet/2}$.

(c) Betti numbers: suppose X is the reduction of a smooth projective variety $\mathcal{X}$ defined over a number ring $\mathcal{O}_K$. Then $\deg P_\bullet = \dim_{\mathbb{C}} H^\bullet(\mathcal{X}(\mathbb{C}), \mathbb{C})$.

We will not bother to explain why $\zeta_X(T)$ is the correct ζ-function to look at (roughly speaking, one is supposed to plug in $T \coloneqq q^{-s}$).

The mention of Betti numbers is rather compelling because it suggests that there ought to be a way to write down a cohomology theory for smooth projective varieties X. Without going into too much detail, let's explain how this is done. It is possible to define a satisfactory cohomology theory called "ℓ-adic cohomology" which takes as input an auxiliary prime ℓ which is nonzer in $\mathbb{F}_q$ and then is able to (functorialy) produce cohomology groups $H^\bullet(X, \mathbb{Q}_\ell)$ which are $\mathbb{Q}_\ell$-vector spaces. For example, in the situation of Theorem 20(c),

we find that

$$\dim_{\mathbb{Q}_\ell} H^\bullet(X, \mathbb{Q}_\ell) = \dim_{\mathbb{C}} H^\bullet(\mathcal{X}(\mathbb{C}), \mathbb{C}).$$

Now, for Theorem 20, the main point is to be able to compute $\#X(\mathbb{F}_q)$. Well, the main idea is that $X(\mathbb{F}_q)$ consists of the elements of $X(\overline{\mathbb{F}_q})$ which are fixed by the Frobenius morphism $\mathrm{Frob}_q \colon \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}$. Thus, one can use the Lefschetz trace formula on our cohomology theory $H^\bullet(X, \mathbb{Q}_\ell)$ to find

$$\#X(\mathbb{F}_q) = \sum_{i=0}^{2d} (-1)^i \operatorname{tr}\left(\mathrm{Frob}_q | H^i(X, \mathbb{Q}_\ell)\right).$$

Properties of the cohomology theory are then enough to prove the Weil conjectures purely formally.

For example, in the case of a curve C, we find that

$$\#C(\mathbb{F}_q) = q + 1 - \operatorname{tr}\left(\mathrm{Frob}_q | H^1(C, \mathbb{Q}_\ell)\right),$$

so we become interested in the Galois action on some ℓ-adic vector space $H^1(C, \mathbb{Q}_\ell)$. In the following section, we will provide a direct construction for (the dual of) $H^1(E, \mathbb{Q}_\ell)$ for an elliptic curve E.

Exercise 21. Use the above discussion to prove Theorem 13.

1.4 The Tate Module for Elliptic Curves

We now go on the hunt for a Galois representation attached to E, where E continues to be an elliptic curve defined over $\mathbb{Q}$ (with a suitable integral model). It turns out that there basically one way to do this, though the recipe is somewhat roundabout. Something special about E is that it comes with a group law, which means that $E(R)$ is a group (in a functorial way) for all $\mathbb{Q}$-algebras R. For example, Example 8 realized $E(\mathbb{C})$ as $\mathbb{C}/\Lambda$ for some lattice Λ, and the group law on $\mathbb{C}/\Lambda$ is the expected one.

As such, we note that $E(\overline{\mathbb{Q}})$ is a group with an action by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. One can see this purely by the ambient functoriality; alternatively, one can directly construct this action by noting that $E(\overline{\mathbb{Q}}) \subseteq \mathbb{P}^2_{\mathbb{Q}}(\overline{\mathbb{Q}})$, and of course $\mathbb{P}^2_{\mathbb{Q}}(\overline{\mathbb{Q}})$ has a Galois action by acting on the coordinates:

$$\sigma([X : Y : Z]) \coloneqq [\sigma(X) : \sigma(Y) : \sigma(Z)]$$

for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $[X : Y : Z] \in \mathbb{P}^2_{\mathbb{Q}}(\overline{\mathbb{Q}})$.

However, in order to do linear algebra, we want our Galois representation to be valued in a vector space. Thus, the Galois action on $E(\overline{\mathbb{Q}})$ will not quite work. As such, we will want the following fact about the group law; throughout, $G[n]$ denotes the n-torsion of a group G.

Proposition 22. Fix an elliptic curve E defined over an algebraically closed field $\overline{K}$. For any n which is nonzero in K, there is a non-canonical isomorphism

$$E(\overline{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2.$$

Example 23. For $E = \mathbb{C}/\Lambda$, it is not hard to show that $E[n]$ is a group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$. In particular, as abstract groups, one finds that $\mathbb{C} \cong \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$, so

$$E \cong (\mathbb{R}/\mathbb{Z})^2,$$

whose n-torsion has the desired property.

This is slightly better: for any prime ℓ, we see that $E(\overline{\mathbb{Q}})[\ell]$ is a 2-dimensional $\mathbb{F}_\ell$-vector space, and more generally, $E(\overline{\mathbb{Q}})[\ell^\bullet)$ is a free module over $(\mathbb{Z}/\ell^\bullet\mathbb{Z})$ of rank 2. In order to not have to deal with torsion, we take an inverse limit.

Definition 24 (Tate module)**.** Fix an elliptic curve E defined over an algebraically closed field $\overline{K}$. For any prime ℓ nonzero in K, we define the *Tate module* as the inverse limit

$$T_\ell E \coloneqq \varprojlim E\left[\ell^\bullet\right],$$

where the transition maps $E\left[\ell^{\bullet+1}\right] \twoheadrightarrow E\left[\ell^\bullet\right]$ are given by multiplication by ℓ. We also define $V_\ell E \coloneqq T_\ell E \otimes_{\mathbb{Z}} \mathbb{Q}$.

Remark 25. We see that $T_\ell E$ is non-canonically isomorphic to $\mathbb{Z}_\ell^2$, so $V_\ell E$ is non-canonically isomorphic to $\mathbb{Q}_\ell^2$.

Remark 26. Intuitively, one should think about $T_\ell E$ as a complex-analytic version of $H_1(E,\mathbb{Z})$. For example, $(V_\ell E)^\vee$ should be analogous to $H^1(E,\mathbb{Q})$.

The Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on each $E(\overline{\mathbb{Q}})\left[\ell^\bullet\right]$ will now assemble into a Galois action on $T_\ell E$ and thus $V_\ell E$, so we have produced a homomorphism

$$\rho_\ell \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V_\ell E).$$

It is rather difficult to compute this Galois representation directly, but it knows quite a bit about the arithmetic of E.

Proposition 27. Fix an elliptic curve E defined over a field K, and let ℓ be a prime nonzero in K. For any endomorphism $\varphi \colon E \to E$, let $P_\ell(T)$ be the monic characteristic polynomial of φ acting on $V_\ell E$. For each $n \in \mathbb{Z}$, the number $P_\ell(n)$ is independent of ℓ and equals the degree of the map $\varphi - [n]$, where $[n] \colon E \to E$ is multiplication by n.

Example 28. Let's compare this with what we expect to happen for $H_1(E,\mathbb{Z})$ when $E = \mathbb{C}/\Lambda$. Then $H_1(E,\mathbb{Z}) = \Lambda$, so the characteristic polynomial P_φ of some endomorphism $\varphi \colon E \to E$ will satisfy

$$\begin{aligned}
|P_\varphi(n)| &= |\det(\varphi - [n] | H_1(E,\mathbb{Z}))| \\
&= |\det(\varphi - [n] | \Lambda)| \\
&= \#\left(\frac{\Lambda}{(\varphi-[n])\Lambda}\right) \\
&= \#\left(\frac{(\varphi-[n])^{-1}\Lambda}{\Lambda}\right) \\
&= \#\ker(\varphi - [n]) \\
&= \deg(\varphi - [n]).
\end{aligned}$$

Here are two examples.

Corollary 29. Fix an elliptic curve E defined over $\mathbb{Q}$ with a good enough integral model, and let ℓ be a prime. For a prime $p \neq \ell$, let $P_\ell(T)$ be the characteristic polynomial of $\rho_\ell(\mathrm{Frob}_p)$, for any choice of Frob_p in the conjugacy class of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then

$$P_\ell(0) = p \qquad \text{and} \qquad P_\ell(1) = \#E(\mathbb{F}_p).$$

Proof. Let $F \colon A(\overline{\mathbb{F}_p}) \to A(\overline{\mathbb{F}_p})$ be given by the action of Frob_p. Proposition 27 tells us that $P_\ell(0)$ equals the degree of F, which is p because it corresponds to the degree of some field extension which looks like $K(t^p) \subseteq K(t)$. Similarly, we see $P_\ell(1)$ equals the degree of the map $F - \mathrm{id}_E$, which is the number of points fixed by F, which is the size of $E(\mathbb{F}_p)$. ∎

In particular, in the situation of the corollary, we are able to compute that

$$P_\ell(T) = T^2 - aT + p,$$

where $a = (p+1) - \#E(\mathbb{F}_p)$. Factoring $P_\ell(T) = (T-\alpha_1)(T-\alpha_2)$, we find that

$$\frac{1}{\sqrt{p}} \operatorname{tr} \rho_\ell(\mathrm{Frob}_p) = \frac{\alpha_1 + \alpha_2}{\sqrt{p}} = \frac{(p+1) - \#E(\mathbb{F}_p)}{\sqrt{p}} = a_p(E).$$

Thus, our Galois representation is good enough to understand our desired numbers $a_p(E)$!

1.5 Defining the Sato–Tate Group: Elliptic Curves

We continue with our elliptic curve E defined $\mathbb{Q}$, and we fix our auxiliary prime ℓ. The moral of the story is that we can measure the distribution of $a_p(E)$s via the distribution of $\rho_\ell(\mathrm{Frob}_p)$; we then recover the distribution of the $a_p(E)$s by taking the trace.

Once again, we may guess that the $\rho_\ell(\mathrm{Frob}_p)$s must equidistribute in $\mathrm{GL}(V_\ell E) \cong \mathrm{GL}_2(\mathbb{Q}_\ell)$. However, this cannot be the case because

$$\det \rho_\ell(\mathrm{Frob}_p) = p$$

by Corollary 29. Thus, we would like to rescale $\rho_\ell(\mathrm{Frob}_p)$ to account for this determinant condition. Namely, we would like to replace $\rho_\ell(\mathrm{Frob}_p)$ with $\frac{1}{\sqrt{p}}\rho_\ell(\mathrm{Frob}_p)$, but there is no reasonable way to do this because $\mathbb{Q}_\ell$ may not have the element $1/\sqrt{p}$ for all the primes p we want to look at. And even when it does, there are two reasonable square roots to look at, so it is not obvious which one to choose: a different choice will lead to a different trace!

To fix this problem, we cheat: we choose any embedding $\iota\colon \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$, which exists because these two fields have the same cardinality, and $\mathbb{C}$ is algebraically closed. Then we may hope that the elements

$$\frac{1}{\sqrt{p}}\iota(\rho_\ell(\mathrm{Frob}_p)) \in \mathrm{SL}_2(\mathbb{C})$$

will equidistribute as p varies. However, this still cannot be the case because ρ_ℓ is a continuous map with compact source $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so these elements should actually live in some compact group. As such, we fix the compact subgroup $\mathrm{SU}_2 \subseteq \mathrm{SL}_2(\mathbb{C})$, and we hope that the elements

$$\frac{1}{\sqrt{p}}\iota(\rho_\ell(\mathrm{Frob}_p)) \in \mathrm{SU}_2$$

will equidistribute. Technically, this does not really make sense because Frob_p was only defined up to conjugacy, so the element $\frac{1}{\sqrt{p}}\iota(\rho_\ell(\mathrm{Frob}_p))$ will also only be defined up to conjugacy, so we are really hoping that the elements

$$\left[\frac{1}{\sqrt{p}}\iota(\rho_\ell(\mathrm{Frob}_p))\right] \in \mathrm{Conj}(\mathrm{SU}_2)$$

will equidistribute.

This is generally true.

Example 30. For the curve $E_2\colon y^2 = x^3 + x + 1$, it will turn out that the conjugacy classes

$$\left[\frac{1}{\sqrt{p}}\iota(\rho_\ell(\mathrm{Frob}_p))\right] \in \mathrm{Conj}(\mathrm{SU}_2)$$

do equidistribute in $n\,\mathrm{Conj}(\mathrm{SU}_2)$. This is the "generic" case for our elliptic curves, and one can show that this equidistribution gives rise to the semicircle distribution seen in Example 18 upon applying the trace.

In fact, one has the following.

Theorem 31 (Sato–Tate, non-CM elliptic curve)**.** Fix an elliptic curve E defined over $\mathbb{Q}$, and let ℓ be an auxiliary prime, and let $\iota\colon \mathbb{Q}_\ell \to \mathbb{C}$ be some embedding. Let ρ_ℓ be the Galois representation given by $V_\ell E$. Assume $\mathrm{End}(E_{\overline{\mathbb{Q}}}) = \mathbb{Z}$. Then the elements

$$\left\{\frac{1}{\sqrt{p}}\iota(\rho_\ell(\mathrm{Frob}_p))\right\}_{p \text{ prime}}$$

equidistribute among the conjugacy classes of SU_2.

Remark 32. Perhaps we ought to explain what it means to equistribute in $\mathrm{Conj}(\mathrm{SU}_2)$. Well, SU_2 is a compact topological group, so it has a Haar measure, and there is a procedure to push this measure forward along the canonical projection.

The difference between Examples 17 and 18 imply that we cannot expect the above discussion to be true for all elliptic curves.

To explain what is going on, note that $E_1\colon y^2 = x^3 + 1$ has a bizarre extra endomorphism $\varphi\colon E_1 \to E_1$ given by

$$\varphi(x, y) \coloneqq (\zeta_3 x, y).$$

This endomorphism is defined over $\mathbb{Q}(\zeta_3)$, which means that whenever $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_3))$, we will have

$$\rho_\ell(\varphi) \circ \rho_\ell(\mathrm{Frob}_p) = \rho_\ell(\mathrm{Frob}_p) \circ \rho_\ell(\varphi).$$

Thus, we do not expect our elements to equidistribute in $\overline{\mathrm{SU}_2}$: there should be an extra condition to account for commuting with endomorphisms (possibly defined over an extension of $\mathbb{Q}$).

The general way to account for this is to simply ignore it. We have the following definition.

Definition 33 (ℓ-adic monodromy group)**.** Fix an elliptic curve E defined over $\mathbb{Q}$, and let ℓ be an auxiliary prime. Let G_ℓ be the image of ρ_ℓ, and let G_ℓ^{Zar} be the smallest algebraic subgroup of $\mathrm{GL}_2(\mathbb{Q}_\ell)$ which is defined over $\mathbb{Q}_\ell$ containining G_ℓ. We call G_ℓ^{Zar} the *ℓ-adic monodromy group*.

We can now define the Sato–Tate group $\mathrm{ST}(E)$ by retelling the above story.

Definition 34 (Sato–Tate group)**.** Fix an elliptic curve E defined over $\mathbb{Q}$, and let ℓ be an auxiliary prime. Let $G_\ell^{\mathrm{Zar},1}$ be the subgroup of G_ℓ^{Zar} cut out by the condition that the determinant equals 1. Then the *Sato–Tate group* is a maximal compact subgroup of $G_\ell^{\mathrm{Zar},1}(\mathbb{C})$, where we take $\mathbb{C}$-points via some embedding $\mathbb{Q}_\ell \subseteq \mathbb{C}$.

And here is the theorem, due to Richard Taylor and many other people.

Theorem 35 (Sato–Tate, elliptic curve)**.** Fix an elliptic curve E defined over $\mathbb{Q}$, and let ℓ be an auxiliary prime, and let $\iota\colon \mathbb{Q}_\ell \to \mathbb{C}$ be some embedding. Then the elements

$$\left\{\frac{1}{\sqrt{p}}\iota(\rho_\ell(\mathrm{Frob}_p))\right\}_{p \text{ prime}}$$

equidistribute among the conjugacy classes of $\mathrm{ST}(E)$.

Remark 36. It is not totally clear why $\frac{1}{\sqrt{p}}\iota(\rho_\ell(\mathrm{Frob}_p))$ would even be conjugate to any element in $\mathrm{ST}(E)$. Roughly speaking, we are combining two properties.

1. It turns out that $\rho_\ell(\mathrm{Frob}_p)$ is diagonalizable over an algebraic closure. Thus, our element (with eigenvalues of absolute value 1) it certainly contained in some compact subgroup.
2. Over $\mathbb{C}$, it turns out that any compact subgroup is conjugate to a subgroup of a given maximal compact subgroup. Thus, we can conjugate our element into $\mathrm{ST}(E)$.

Example 37. For E_1, one shows that $\mathrm{ST}(E_1)$ is a normalizer of U_1 diagonally embedded in SU_2. Roughly speaking, the point is that the field $\mathbb{Q}(\zeta_3)$ has an action on $V_\ell E_1$ which commutes with the Galois action restricted to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_3))$, which causes the Galois action to diagonalize.

1.6 The Sato–Tate Conjecture: Abelian Varieties

In order to wrap up our story, we note that our discussion of Sato–Tate groups for elliptic curves generalizes to abelian varieties without too much effort.

Definition 38 (abelian variety)**.** Fix a field K. Then an *abelian variety* A over K is a smooth projective geometrically integral group variety over K.

Here, being a group variety means that $A(R)$ is a group (in a functorial way) for all K-alegbras R, as we had for elliptic curves.

Example 39. Any product of elliptic curves continues to be an abelian variety. The category of abelian varieties is in fact abelian, so we can also take kernels and cokernels.

Example 40. Fix a nonnegative integer g. Then for some lattices $\Lambda \subseteq \mathbb{C}^g$, it turns out that the quotient $\mathbb{C}^g/\Lambda$ is a projective variety over $\mathbb{C}$, so this is an abelian variety over $\mathbb{C}$ with the obvious group law.

Let's make explicit how the discussion of the previous two subsections generalizes to abelian varieties. Here is the generalization of Proposition 22.

Proposition 41. Fix an abelian vareity A over a field K of dimension g. For any n which is nonzero in K, there is a non-canonical isomorphism

$$A(\overline{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

This allows us to define the Tate module as before.

Definition 42 (Tate module)**.** Fix an abelian variety A defined over a field K. For any prime ℓ nonzero in K, we define the *Tate module* as the inverse limit

$$T_\ell A \coloneqq \varprojlim A\left[\ell^\bullet\right].$$

We also define $V_\ell A \coloneqq T_\ell A \otimes_{\mathbb{Z}} \mathbb{Q}$. As before, we find that $T_\ell A$ is a free module over $\mathbb{Z}_\ell$ of rank $2g$.

Thus, as before, we get an ℓ-adic Galois representation

$$\rho_\ell \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V_\ell A).$$

We can also generalize some of our discussion about the characteristic polynomial. Here is the generalization of Corollary 29.

Proposition 43. Fix an abelian variety A defined over $\mathbb{Q}$ with a good enough integral model, and let ℓ be a prime. For a prime $p \neq \ell$, let $P_\ell(T)$ be the characteristic polynomial of $\rho_\ell(\mathrm{Frob}_p)$, for any choice of Frob_p in the conjugacy class of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then $P_\ell(T)$ is a polynomial independent of ℓ, and

$$P_\ell(0) = p^g \qquad \text{and} \qquad P_\ell(1) = \#A(\mathbb{F}_p).$$

Thus, our discussion defining $\mathrm{ST}(E)$ can be generalized to build $\mathrm{ST}(A)$, as follows.

1. Let $G_\ell(A)$ be the image of ρ_ℓ in $\mathrm{GL}(V_\ell A)$, and let $G_\ell^{\mathrm{Zar}}(A)$ be the smallest algebraic subgroup defined over $\mathbb{Q}_\ell$ containing G_ℓ.
2. By choosing a Weil pairing on $T_\ell A$ (which we will not define), it turns out that there is a non-degenerate symplectic form on $V_\ell A$, and $\rho_\ell(\mathrm{Frob}_p)$ acts with multiplier p with respect to this form. Thus, we let $G_\ell^{\mathrm{Zar},1}(A)$ be the subgroup of $G_\ell^{\mathrm{Zar}}(A)$ cut out by preserving the corresponding symplectic form.
3. Choose some embedding $\iota\colon \mathbb{Q}_\ell \to \mathbb{C}$. We now let $\mathrm{ST}(A)$ be a maximal compact subgroup of the complex algebraic group $\iota\left(G_\ell^{\mathrm{Zar},1}(A)\right)$.

And here is the conjecture.

Conjecture 44 (Sato–Tate)**.** Fix an abelian variety A defined over $\mathbb{Q}$, and let ℓ be an auxiliary prime, and let $\iota\colon \mathbb{Q}_\ell \to \mathbb{C}$ be some embedding. Let ρ_ℓ be the Galois representation given by $V_\ell A$. Then the elements

$$\left\{ \frac{1}{\sqrt{p}} \iota(\rho_\ell(\mathrm{Frob}_p)) \right\}_{p \text{ prime}}$$

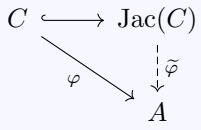
equidistribute among the conjugacy classes of $\mathrm{ST}(A)$.

Remark 36 once again explains why our elements have a conjugacy class in $\mathrm{ST}(A)$. Also, note that this is a conjecture unlike Theorem 35!

1.7 Jacobian Varieties

In order to provide some examples of abelian varieties, we introduce Jacobian varieties into our story. In order to avoid doing any difficult algebraic geometry or complex geometry, we will define these by universal property.

Proposition 45. Fix a curve C defined over a field K equipped with a point $x \in C(K)$. Then there exists an abelian variety $\mathrm{Jac}(C)$ equipped with a map $C \hookrightarrow \mathrm{Jac}(C)$ sending $x \mapsto 0$ and satisfying the following the corresponding universal property: for any abelian variety A and morphism $\varphi\colon C \to A$ sending $\varphi(x) = 0$, there exists a unique map $\widetilde{\varphi}\colon \mathrm{Jac}(C) \to A$ making the following diagram commute.



Definition 46 (Jacobian)**.** Fix a curve C defined over a field K equipped with a point $x \in C(K)$. Then the abelian variety $\mathrm{Jac}(C)$ produced by Proposition 45 is called the *Jacobian* of C.

Example 47. For an elliptic curve E, we see that $\mathrm{Jac}(E) = E$ because E is already an abelian variety.

Example 48. Let's give the construction for $\mathrm{Jac}(C)$ when our curve C is defined over $\mathbb{C}$. One can embed the first homology $H_1(C,\mathbb{Z})$ into the complex vector space $H^0(C,\Omega^1_C)^\vee$ by taking $[\gamma] \in H_1(C,\mathbb{Z})$ to the functional

$$\omega \mapsto \int_\gamma \omega.$$

Then $\mathrm{Jac}(C) = H^0(C,\Omega^1_C)^\vee / H_1(C,\mathbb{Z})$.

Remark 49. It is not obvious from the definition, but it turns out that the dimension of $\mathrm{Jac}(C)$ equals the genus of the curve C.

Remark 50. Motivated by section 1.3, the importance of the Jacobian arises from the fact that the map $C \to \mathrm{Jac}(C)$ induces an isomorphism

$$H^1(\mathrm{Jac}(C),\mathbb{Q}_\ell) \to H^1(C,\mathbb{Q}_\ell)$$

on first cohomology. In particular, we can hope to read off properties of the curve (related to its cohomology) from the Jacobian. The analogous statement for $\mathbb{C}$ is simply that $H_1(C,\mathbb{Z}) \to H_1(\mathrm{Jac}(C),\mathbb{Z})$ is an isomorphism, which is clear from our construction.

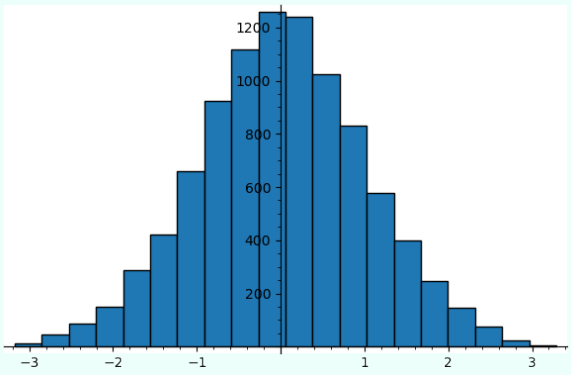
The following result follows from the discussion in section 1.3 and the above remark.

Proposition 51. Fix a curve C defined over $\mathbb{Q}$ with a good enough integral model, and set $A := \mathrm{Jac}(C)$. For any prime p and an auxiliary prime $\ell \neq p$, we have

$$\#C(\mathbb{F}_p) - (p+1) = \mathrm{tr}\,(\rho_\ell(\mathrm{Frob}_p)|V_\ell A)$$

Thus, we expect computable (but perhaps complicated) equidistribution results for general curves to follow from Conjecture 44. Here is one such histogram.

Example 52. Consider the genus-2 curve $C\colon y^2 = x^5 + x + 1$. Here is a histogram for the values of $a_p(C) := (\#C(\mathbb{F}_p) - (p+1))/\sqrt{p}$ for $p < 10^5$.



2 CM Theory

In our second talk, we will use the theory of complex multiplication to discuss how to compute $\mathrm{ST}(A)$ for certain abelian varieties A.

2.1 Algebraic Tori

In this subsection, we recall some facts about algebraic tori.

Definition 53 (algebraic torus)**.** Fix a field k with separable closure k^{sep}. Then an *algebraic torus* is a connected algebraic group scheme T over k such that $T_{k^{\mathrm{sep}}} \cong \mathbb{G}_{m,k^{\mathrm{sep}}}^r$ for some $r \geq 0$; we say that r is the *rank* of T, sometimes denoted $\mathrm{rank}(T)$.

Remark 54. Importantly, the isomorphism $T \cong \mathbb{G}_m^r$ need note be defined over k.

Example 55 (Deligne torus)**.** Consider the group $\mathbb{S} \coloneqq \mathrm{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{G}_{m,\mathbb{C}}$, which is an algebraic group defined over $\mathbb{R}$ such that $\mathbb{S}(\mathbb{R}) \cong \mathbb{C}^\times$. Explicitly, we can write

$$\mathbb{S}(R) = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in M_2(R) : a^2 + b^2 \in R^\times \right\},$$

for any $\mathbb{R}$-algebra R. Then one can check that $\mathbb{S}(\mathbb{C}) \cong \mathbb{C}^\times \times \mathbb{C}^\times$, which actually assembles into an isomorphism of algebraic groups

$$\mathbb{S}_{\mathbb{C}} \cong \mathbb{G}_{m,\mathbb{C}} \times \mathbb{G}_{m,\mathbb{C}}.$$

Example 56. More generally, for any finite separable field extension E/F, one can define a torus $T_{E/F} \coloneqq \mathrm{Res}_{E/F} \mathbb{G}_{m,E}$, and then one finds that $T_{E/F} \otimes_F E \cong \mathbb{G}_{m,E}^{[E:F]}$. Roughly speaking, one upgrades the isomorphism

$$E \otimes_F F^{\mathrm{sep}} \cong E^{\mathrm{Hom}(E,F^{\mathrm{sep}})}$$

to an isomorphism of algebraic groups. (This isomorphism uses the primitive element theorem, which is why E/F is required to be separable.)

Given a torus T, we define the groups

$$X^*(T) \coloneqq \mathrm{Hom}(T_{k^{\mathrm{sep}}}, \mathbb{G}_m) \qquad \text{and} \qquad X_*(T) \coloneqq \mathrm{Hom}(\mathbb{G}_m, T_{k^{\mathrm{sep}}}),$$

which are the character and cocharacter groups, respectively. Because $T_{k^{\mathrm{sep}}} \cong \mathbb{G}_m^r$ for some $r \geq 0$, we see that these are both free abelian groups with rank r. However, there is also an important Galois action by $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ on both of these groups via its action on $T_{k^{\mathrm{sep}}}$.

Example 57. We can define two characters $\mathbb{S}_{\mathbb{C}} \to \mathbb{G}_m$ given on points

$$\mathbb{C}^\times = \mathbb{S}(\mathbb{R}) \subseteq \mathbb{S}(\mathbb{C}) \to \mathbb{G}_m(\mathbb{C})$$

by $z \mapsto z$ and $z \mapsto \overline{z}$. One can check that these two characters span $X^*(\mathbb{S})$, and the nontrivial Galois action of complex conjugation in $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ simply swaps these two characters.

Example 58. Similarly, fix a number field E, and consider the torus $T_E \coloneqq \mathrm{Res}_{E/\mathbb{Q}} \mathbb{G}_m$. For each $\varphi \in \mathrm{Hom}(E, \overline{\mathbb{Q}})$, define we define a character of T_E given by projection onto the φ coordinate in the isomorphism

$$E \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \cong \overline{\mathbb{Q}}^{\mathrm{Hom}(E,\overline{\mathbb{Q}})}$$

of algebras with Galois action. In this way, we find that $X^*(T_E) = \mathbb{Z}[\mathrm{Hom}(E, \mathbb{C})]$, which is an isomorphism of Galois modules. Note that one can then construct a dual basis $\varphi^\vee$ of $X_*(T_E)$.

The importance of the character group is the following result.

Theorem 59. Fix a field k. The contravariant functor X_* defines an anti-equivalence of categories between the category of algebraic tori (over k) and free abelian groups of finite rank which are $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-modules.

Remark 60. There is an analogous result for the covariant functor X_*.

Roughly speaking, the idea is that (over k^{sep}) one can understand tori perfectly by their maps to $\mathbb{G}_m$ because one really only cares about rank. To descend to k, one then needs to keep track of the Galois action.

2.2 A Little Hodge Theory

Before doing anything too intense, we will discuss some Hodge theory.

Definition 61 (Hodge structure)**.** Fix an integer n. A *Hodge structure* over $\mathbb{Q}$ is a $\mathbb{Q}$-vector space equipped with a decomposition

$$V_{\mathbb{C}} = \bigoplus_{(p,q)\in\mathbb{Z}^2} V^{p,q}$$

such that $V^{p,q} = \overline{V^{q,p}}$. If $V^{p,q} \neq 0$ only when $p+q=n$, then we say that V is *pure of weight* n.

Remark 62. There is also a notion of an integral Hodge structure, where we make $\mathbb{Z}$ into a free $\mathbb{Z}$-module instead of a $\mathbb{Q}$-vector space.

Here is the key example.

Example 63. Fix a smooth proper complex variety X over $\mathbb{C}$. Then the cohomology group $H^n(X(\mathbb{C}),\mathbb{Q})$ admits a Hodge decomposition as

$$H^n(X(\mathbb{C}),\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} = \bigoplus_{p+q=n} H^{p,q},$$

where $H^{q,p} = H^q(X(\mathbb{C}), \Omega^p_{X/\mathbb{C}})$.

Example 64. We are interested in abelian varieties A. Then all cohomology is generated by H^1, so it will be enough to understand the Hodge structure there. Thus, for an abelian variety A, we note that there is a Hodge structure on $H_1(A,\mathbb{Q})$ of weight -1. (The weight negates because we are now looking at homology.)

Intuitively, Hodge theory is the extra structure on cohomology provided by complex geometry, in the same way that Galois theory is the extra structure on cohomology provided by the étale site.

The reason we are bringing up this Hodge theory is that we will be able to compute the complex analytic version of the ℓ-adic monodromy group $G_\ell(A)$. For this, we will need a representation-theoretic interpretation of a Hodge structure.

Lemma 65. Fix a vector space V defined over $\mathbb{Q}$. The data of a Hodge structure on V is equivalent to the data of a representation $h\colon \mathbb{S} \to \mathrm{GL}(V_{\mathbb{R}})$.

Proof. The point is to describe what representations look like. Over $\mathbb{S}_{\mathbb{C}}$, we see that the representation h will diagonalize as a representation $\mathbb{G}^2_{m,\mathbb{C}} \to \mathrm{GL}(V_{\mathbb{C}})$. Thus, we can decompose

$$V_{\mathbb{C}} = \bigoplus_{\chi\in X^*(\mathbb{S})} V_\chi,$$

where V_χ is the χ-eigenspace. Now, each character χ can be written as $z \mapsto z^{-p}\overline{z}^{-q}$ for some $(p,q) \in \mathbb{Z}^2$ where $z, \overline{z} \in X^*(\mathbb{S})$ are the characters of Example 57, so we let $V^{p,q}$ be the eigenspace for this character. As such, we see that the nontrivial Galois action of complex conjugation in $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ will swap $V^{p,q}$ and $V^{q,p}$, so $V^{p,q} = \overline{V^{q,p}}$. Thus, we see that we have produced a Hodge structure on V; one can then reverse this construction to produce a representation of $\mathbb{S}$ from any given Hodge structure. ■

Now that we have a representation, we can take monodromy.

Definition 66 (Mumford–Tate group)**.** Fix a Hodge structure over $\mathbb{Q}$ on a vector space V. Then the *Mumford–Tate group* $\mathrm{MT}(V)$ is the smallest connected algebraic group defined over $\mathbb{Q}$ containing the image of $h\colon \mathbb{S} \to \mathrm{GL}(V_\mathbb{R})$. For brevity, given an abelian variety A defined over $\mathbb{C}$, we may write $\mathrm{MT}(A)$ for the Mumford–Tate group of the Hodge structure on $H_1(A,\mathbb{Q})$.

Remark 67. There is also an important Tannakian definition of $\mathrm{MT}(V)$. In short, the category of Hodge structures over $\mathbb{Q}$ is neutral Tannakian, so for any Hodge structure V, we can look at the Tannakian subcategory generated by V. Then $\mathrm{MT}(V)$ is the algebraic group given by this category.

Remark 68. Because an algebraic group can be described by the vectors it fixes, the above definition can be restated as follows: $\mathrm{MT}(V)$ is the subgroup such that a rational subquotient W of some sum of Vs and $V^\vee$s is a Hodge substructure if and only if W. For example, this allows one to see that $\mathrm{MT}(V) \subseteq \mathrm{GL}(V)$ must contain the scalar matrices.

Remark 69. For an abelian variety A, it turns out that $\mathrm{MT}(A)$ is always reductive. Roughly speaking, this follows from the fact that A has a polarization, so $H_1(A,\mathbb{Q})$ is a polarizable Hodge structure.

It is at this point that one would expect me to write down some basic examples of Mumford–Tate groups, but this turns out to be a fairly difficult task. For example, because we are looking at the image of some torus $\mathbb{S}$, one may expect that $\mathrm{MT}(V)$ is frequently a torus. In our application (in the CM theory), this will turn out to be the case, but this is exceptional: most of the time we expect $\mathrm{MT}(V)$ to be large (largely because the algebraic group needs to descend all the way $\mathbb{Q}$), though this is not always easy to prove.

Nonetheless, let us give a couple remarks bounding $\mathrm{MT}(A)$.

Remark 70. For brevity, set $V \coloneqq H_1(A,\mathbb{Q})$ and $D \coloneqq \mathrm{End}(A) \otimes_\mathbb{Z} \mathbb{Q}$, which one can show is a product of division algebras over $\mathbb{Q}$. It turns out that endomorphisms of A then correspond to endomorphisms of V preserving the Hodge structure. However, an endomorphism of V preserving the Hodge structure turns out to be the same data of an element of $V \otimes V^\vee$ which is fixed by the image of h, which of course is equivalent to being fixed by $\mathrm{MT}(A)$. Thus, we see that

$$\mathrm{End}(V)^{\mathrm{MT}(A)} = \mathrm{End}(A).$$

Thus, we see that we have a lower bound that $\mathrm{MT}(A)$ will be contained with the subgroup of $\mathrm{GL}(V)$ commuting with the action of D.

Remark 71. Once again, set $V \coloneqq H_1(A,\mathbb{Q})$. Let $\psi\colon V \times V \to \mathbb{C}$ be the polarization, which is some symplectic form. Then ψ as a polarization actually defines a class in $(V \otimes V)^\vee$ preserved by the action of h. Thus, we see that $\mathrm{MT}(A)$ must preserve this polarization, so we conclude that

$$\mathrm{MT}(A) \subseteq \mathrm{GSp}(V,\psi).$$

We conclude with the following conjecture, which explains why we have introduced $\mathrm{MT}(V)$.

Conjecture 72 (Mumford–Tate)**.** Fix an abelian variety A defined over $\mathbb{Q}$. For any auxiliary prime ℓ, we have

$$\mathrm{MT}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = G_\ell(A)^\circ.$$

Remark 73. This conjecture is known in many, many cases; for example, it is known when A has complex multiplication, a notion we will review in the next subsection.

The point of this is that one can compute $\mathrm{MT}(A)$ instead of $G_\ell(A)^\circ$. This allows us to compute $\mathrm{ST}(A)^\circ$ by taking a maximal compact subgroup of $\mathrm{MT}(A)_{\mathbb{C}}$. In order to get understand the full group $\mathrm{ST}(A)$, one still needs to understand some Galois action which is only visible in the ℓ-adic side, but computing $\mathrm{ST}(A)^\circ$ is still a good start, and we will content ourselves with these computations for today.

2.3 Complex Multiplication

The key notion for today's talk is that of an abelian variety with complex multiplication.

Definition 74 (CM)**.** A *CM field* is a number field E is CM if and only if it is a totally imaginary quadratic extension of a totally real field. A *CM algebra* is a product of CM fields.

Example 75. Any imaginary quadratic field is CM, such as $\mathbb{Q}(i)$.

Example 76. For any $n \geq 3$, we see that the cyclotomic field $\mathbb{Q}(\zeta_n)$ is a CM field because it is a totally imaginary quadratic extension of the totally real field $\mathbb{Q}\left(\zeta_n + \zeta_n^{-1}\right) = \mathbb{Q}\left(\cos \frac{2\pi}{n}\right)$.

Remark 77. One can show that the Galois closure of any CM algebra is still a CM algebra.

Definition 78 (CM abelian variety)**.** Fix an abelian variety A defined over a number field. Then A has *CM* or *complex multiplication* if and only if there is a CM algebra E such that $[E : \mathbb{Q}] = 2 \dim A$ and

$$\mathrm{End}(A_{\mathbb{C}}) \otimes_{\mathbb{Z}} \mathbb{Q} = E.$$

Remark 79. It turns out that having CM is equivalent to

$$\dim_{\mathbb{Q}} \mathrm{End}(A_{\mathbb{C}}) \otimes_{\mathbb{Z}} \mathbb{Q} \geq 2g.$$

Namely, if this inequality is satisfied, then one can show that equality actually holds and that $\mathrm{End}(A_{\mathbb{C}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a CM algebra.

Example 80. Consider the elliptic curve $E_1 : y^2 = x^3 + 1$. Then $(E_1)_{\mathbb{C}}$ has an order-three endomorphism given on points by

$$(x, y) \mapsto (\zeta_3 x, y).$$

In this way, we find that $\mathbb{Q}(\zeta_3) \subseteq \mathrm{End}(E_{\mathbb{C}}) \otimes_{\mathbb{Z}} \mathbb{Q}$, so E_1 has CM by $\mathbb{Q}(\zeta_3)$.

Example 81. Fix a prime p and integer $a \in \{1, 2, \dots, p-1\}$, and consider the superelliptic curve $C\colon y^p = x^a(x-1)$. (It turns out that this curve is a quotient of the curve $x^p + y^p = 1$, so C is sometimes called a "Fermat curve.") A computation with the Riemann–Hurwitz formula shows $\dim C = \frac{p-1}{2}$, so $\dim \mathrm{Jac}(C) = \frac{p-1}{2}$. On the other hand, we see that C has an automorphism of order p given by

$$(x, y) \mapsto (x, \zeta_p y),$$

so $\mathbb{Q}(\zeta_p) \subseteq \mathrm{End}(\mathrm{Jac}(C)_{\mathbb{C}}) \otimes_{\mathbb{Z}} \mathbb{Q}$. Thus, $\mathrm{Jac}(C)$ has CM by $\mathbb{Q}(\zeta_p)$.

As in the story of toric varieties, it can be rather hard to believe that the given definition will actually have interesting (and computable) applications. One goal of the present talk is to present some of these results. For example, we begin by noting that $\mathrm{MT}(A)$ is necessarily simple easy in our situation.

Proposition 82. Fix an abelian variety A defined over $\mathbb{C}$. Then A has complex multiplication if and only if $\mathrm{MT}(A)$ is a torus.

Proof. We will use the bound of Remark 70 to show our implications.

- Suppose that A has CM by the CM algebra E. Then we see that E has an action on V, so V becomes a free module of rank 1 over E. Now, $\mathrm{MT}(A)$ needs to commute with this E-action, but after identifying V with E (by choosing a basis as a nonzero vector), we see that the available endomorphisms in $\mathrm{GL}(V)$ are simmply given by $E^\times$. In this way, we find that $\mathrm{MT}(A)$ is contained in the torus $T_E = \mathrm{Res}_{E/\mathbb{Q}} \mathbb{G}_{m,E}$. We conclude that $\mathrm{MT}(A)$ is a torus.
- Suppose that $\mathrm{MT}(A)$ is a torus; choose a maximal torus $T \subseteq \mathrm{GL}(V)$ containing $\mathrm{MT}(A)$. Then

  $$\mathrm{End}(V)^T \subseteq \mathrm{End}(V)^{\mathrm{MT}(A)} = D,$$

  so D contains $\mathrm{End}(V)^T$, which we see (by diagonalizing T) equals a $\mathbb{Q}$-algebra with dimension $2g$. Thus, we are done by Remark 79. ∎

Importantly, if A has CM by E, then the above proof has actually shown that $\mathrm{MT}(A)$ is contained in the explicit torus $\mathrm{Res}_{E/\mathbb{Q}} \mathbb{G}_{m,E}$. We would like to understand the subgroup, so we make the following remark to show that it is not the entire torus, extending Remark 71.

Lemma 83. Fix an abelian variety A defined over $\mathbb{C}$ with complex multiplication by E. As usual, set $V := H_1(A, \mathbb{Q})$, and let $\psi\colon V \times V \to \mathbb{Q}$ be the polarization. For each $\varphi, \varphi' \in \mathrm{Hom}(E, \mathbb{C})$, we have

$$\psi(V_\varphi, V_{\varphi'}) = 0$$

unless $\varphi = \overline{\varphi'}$. Here, V_φ is the φ-eigenspace for the E-action on $V_{\mathbb{C}}$.

Proof. Quickly, recall that having CM means that V is a free module of rank 1 over E, so each $V_{\mathbb{C}} \cong (E \otimes_{\mathbb{Q}} \mathbb{C})$, so $\dim_{\mathbb{C}} V_\varphi = 1$ for each φ. Thus, $\psi(V_\varphi, V_\varphi) = 0$ because ψ is symplectic.

Now, suppose that $\varphi' \notin \{\varphi, \overline{\varphi}\}$. Then φ' and φ remain unequal upon restriction to the maximal totally real subfield of E, so choose some e in this totally real subfield such that $\varphi(e) \neq \varphi'(e)$. Then any $v \in V_\varphi$ and $v' \in V_{\varphi'}$ has

$$\varphi(e)\psi(v, v') = \psi(\varphi(e)v, v') = \psi(ev, v') \overset{*}{=} \psi(v, ev') = \psi(v, \varphi'(e), v') = \varphi'(e)\psi(v, v'),$$

where $\overset{*}{=}$ holds because the polarization commutes with endomorphisms of A. We conclude $\psi(v, v') = 0$. ∎

Proposition 84. Fix an abelian variety A defined over $\mathbb{C}$ with complex multiplication by E. By diagonalizing the action of E on $H_1(A,\mathbb{C})$, choose an eigenbasis $\{v_\varphi : \varphi \in \mathrm{Hom}(E,\mathbb{C})\}$. Then

$$\mathrm{MT}(A) \subseteq \{\mathrm{diag}(\{\lambda_\varphi : \varphi \in \mathrm{Hom}(E,\mathbb{C})\}) : \lambda_\varphi \lambda_{\overline{\varphi}} = \lambda_{\varphi'}\lambda_{\overline{\varphi'}}\}.$$

In particular, $\mathrm{rank}\,\mathrm{MT}(A) \leq \dim A + 1$, with equality holding if and only if the above inclusion is an equality.

Proof. To make sentence of the inclusion, we see that $\mathrm{MT}(A)$ is embedded into $\mathrm{Res}_{E/\mathbb{Q}}\mathbb{G}_{m,E}$, and this group's action diagonalizes with the given eigenbasis $\{v_\varphi\}$ and eigenvalues $\{\varphi\}$.

Now, the main point here is to use a polarization ψ of $V := H_1(A,\mathbb{Q})$. Then we note that $\mathrm{MT}(A)$ is a subset of $\mathrm{GSp}(V,\psi)$ by Remark 71. The above lemma explains that the symplectic space (V,ψ) decomposes into a direct sum of symplectic subspaces $V_\varphi \oplus V_{\overline{\varphi}}$. Now, the given equations are simply asserting that a scalar matrix in $\mathrm{Res}_{E/\mathbb{Q}}\mathbb{G}_{m,E}$ is scaling all these symplectic spaces $V_\varphi \oplus V_{\overline{\varphi}}$ by the same scalar, which is exactly what it means to be in $\mathrm{GSp}(V,\psi)$ upon applying the decomposition of the previous sentence. ∎

Generically speaking, one expects equality in Proposition 84, but exceptions abound.

2.4 Hodge Structures via CM Types

In order to compute the subgroup $\mathrm{MT}(A) \subseteq T_E$, we need to understand the Hodge structure of $H_1(A,\mathbb{Q})$. This is the point of the CM type.

Definition 85 (CM type)**.** Fix an abelian variety A with complex multiplication by E. Note the vector space $H^{10} = H^0(A(\mathbb{C}),\Omega_{A/\mathbb{C}})$ then has an E-action, so it diagonalizes as

$$H^{10} = \bigoplus_{\varphi\in\Phi} \mathbb{C}_\varphi,$$

where $\Phi \subseteq \mathrm{Hom}(E,\mathbb{C})$, and E acts on $\mathbb{C}_\varphi$ via the embedding $\varphi\colon E \to \mathbb{C}$. The *CM type* of A is the subset $\Phi \subseteq \mathrm{Hom}(E,\mathbb{C})$. We may say that A has CM type Φ or (E,Φ).

Remark 86. A priori, one may be worried that

$$H^{10} = \bigoplus_{\varphi\in\Phi} \mathbb{C}_\varphi^{n_\varphi}$$

for some nonnegative integers n_φ, possibly bigger than 1. However, the Hodge decomposition tells us $H^{10} \oplus \overline{H^{10}}$ is isomorphic to $H^1(A,\mathbb{Q})$, which is a vector space of $\mathbb{Q}$-dimension $2\dim A$ and hence a free E-module of rank 1. Thus, we see that $n_\varphi + n_{\overline{\varphi}} = 1$ for each φ, so $n_\varphi \in \{0,1\}$. We also conclude that

$$\{\varphi : \varphi \in \Phi\} \sqcup \{\overline{\varphi} : \varphi \in \Phi\} = \mathrm{Hom}(E,\mathbb{C}),$$

where the bar denotes complex conjugation.

The point is that Φ remembers everything about the Hodge decomposition by explaining what H^{10} is. Let's see some examples.

Example 87. Consider the elliptic curve $E_1 \colon y^2 = x^3 + 1$. Then $H^0(E_1, \Omega_{E_1})$ consits of the first-order holomorphic differentials on E_1, which we note is dx/y. Now, $\mathbb{Q}(\zeta_3)$ acts on this differential by sending dx/y to

$$\frac{d(\zeta_3 x)}{y} = \zeta_3 \cdot \frac{dx}{y},$$

so the CM type consists of the single embedding $\mathbb{Q}(\zeta_3) \to \mathbb{C}$ given by $\zeta_3 \mapsto \zeta_3$.

Example 88. Fix a prime p and integer $a \in \{1, 2, \dots, p-1\}$, and consider the curve $C \colon y^p = x^a(x-1)$. Because $H^1(\operatorname{Jac} C, \mathbb{Q}) = H^1(C, \mathbb{Q})$, we can compute the CM type on $\operatorname{Jac} C$ by computing $H^0(C, \Omega_C)$. Well, one can compute a basis of holomorphic differentials on this curve C. Letting $\varphi_r \in \operatorname{Hom}(\mathbb{Q}(\zeta_p), \mathbb{C})$ be the embedding given by $\varphi_r \colon \zeta_p \mapsto \zeta_p^r$, one finds that the CM type is

$$\{\varphi_r : \langle r \rangle + \langle ra \rangle < p\},$$

where $\langle \bullet \rangle$ refers to the $\pmod p$ representative in $\{0, 1, \dots, p-1\}$. For example, if $a = 1$, our CM type is $\{\varphi_1, \dots, \varphi_{(p-1)/2}\}$.

Because $\mathrm{MT}(A)$ only depends on this Hodge structure, we can now profit.

Proposition 89. Fix an abelian variety A with CM type (E, Φ), and embed $\mathrm{MT}(A)$ into $\operatorname{Res}_{E/\mathbb{Q}} \mathbb{G}_{m,E}$. Then $X_*(\mathrm{MT}(A))$ is the smallest saturated $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant sublattice of $X_*(\operatorname{Res}_{E/\mathbb{Q}} \mathbb{G}_{m,E})$ containing

$$\sum_{\varphi \in \Phi} \varphi^\vee.$$

Here, a saturated sublattice means that the corresponding quotient is torsion-free.

Proof. As usual, set $V \coloneqq H_1(A, \mathbb{Q})$. Note that $\mathrm{MT}(A)$ is by definition the smallest algebraic subtorus of $\operatorname{Res}_{E/\mathbb{Q}} \mathbb{G}_{m,E}$ containing the image of the Hodge character $h \colon \mathbb{S}_{\mathbb{C}} \to \mathrm{GL}(V)_{\mathbb{C}}$. For technical reasons, we define the character $\mu \colon \mathbb{G}_{m,\mathbb{C}} \to \mathbb{S}_{\mathbb{C}}$ given on $\mathbb{C}$-points by $\mu(z) \coloneqq (z, 1) \in \mathbb{S}(\mathbb{C})$. Because complex conjugation simply swaps the two coordinates, we see that $\mathrm{MT}(A)$ is also the smallest algebraic subtorus of $\operatorname{Res}_{E/\mathbb{Q}} \mathbb{G}_{m,E}$ containing $h \circ \mu$.

The point of this technical step is that $(h \circ \mu)$ is a bona fide cocharacter $\mathbb{G}_{m,\mathbb{C}} \to \mathrm{MT}(A) \subseteq \operatorname{Res}_{E/\mathbb{Q}} \mathbb{G}_{m,E}$. To compute it, we note that $h(\mu(z))$ acts by multiplication-by-z on $V^{(-1,0)}$ and trivially on $V^{(0,-1)}$, so

$$(\varphi \circ h \circ \mu)(z) = \begin{cases} z & \text{if } \varphi \in \Phi, \\ 1 & \text{if } \varphi \notin \Phi, \end{cases}$$

for any $\varphi \in \operatorname{Hom}(E, \mathbb{C})$ (which is identified with a projection character of $\operatorname{Res}_{E/\mathbb{Q}} \mathbb{G}_{m,E}$). Thus,

$$h \circ \mu = \sum_{\varphi \in \Phi} \varphi^\vee.$$

The equivalence of categories given by X_* tells us that $X_*(\mathrm{MT}(A)) \subseteq X_*(\operatorname{Res}_{E/\mathbb{Q}} \mathbb{G}_{m,E})$ becomes the smallest saturated Galois-invariant sublattice containing the above cocharacter. ∎

It may look like we only have one element spanning $\mathrm{MT}(A)$, but it is important to note that the Galois action will allow us to premute this into many rather different-looking vectors. Let's see an example.

Example 90. Consider the Jacobian of the curve $C\colon y^5 = x(x-1)$. Then Example 88 tells us that our CM type is $\{\varphi_1, \varphi_2\}$. Thus, on applying the Galois action, we see that $X_*(\mathrm{MT}(A))$ is spanned by the vectors

$$\{\varphi_1^\vee + \varphi_2^\vee, \varphi_2^\vee + \varphi_4^\vee, \varphi_3^\vee + \varphi_1^\vee, \varphi_4^\vee + \varphi_3^\vee\}.$$

Thus, upon ordering our basis, we are interested in computing the kernel of the matrix

$$\begin{bmatrix} 1 & & 1 & \\ 1 & 1 & & \\ & & 1 & 1 \\ & 1 & & 1 \end{bmatrix}.$$

This matrix has rank 3 with kernel spanned by the vector $(1,-1,-1,1)$, so we see that

$$\mathrm{MT}(A) = \{\mathrm{diag}(\lambda_1,\lambda_2,\lambda_3,\lambda_4) : \lambda_1\lambda_4 = \lambda_2\lambda_3\}.$$

Note that this equation is explained by the polarization via Proposition 84.

Example 91. Consider the Jacobian of the curve $C\colon y^{67} = x^6(x-1)$. Then one can do a computation similar to the previous example to find that

$$\dim \mathrm{MT}\,\mathrm{Jac}(C) = 66,$$

which is two smaller than the expected generic case described in Proposition 84.

We will generalize Example 90 in the next subsection.

2.5 The Rank of a CM Type

Proposition 89 tells us that we can compute $\mathrm{MT}(A)$ combinatorially from the CM type. In this subsection, we gather some tools to understand this combinatorics. We begin with a more general definition of CM type.

Definition 92 (CM type)**.** Fix a CM algebra E. Then a *CM type* is a subset $\Phi \subseteq \mathrm{Hom}(E,\mathbb{C})$ such that

$$\{\varphi : \varphi \in \Phi\} \sqcup \{\overline{\varphi} : \varphi \in \Phi\} = \mathrm{Hom}(E,\mathbb{C}).$$

We may call the pair (E,Φ) a CM type.

Definition 93 (rank)**.** Fix a CM type (E,Φ). Then the *rank* of (E,Φ) is the $\mathbb{Q}$-dimension of the image of the map $\mathrm{T}_\Phi\colon E \to \mathbb{C}$ given by

$$\mathrm{T}_\Phi(\alpha) \coloneqq \sum_{\varphi\in\Phi} \varphi(\alpha).$$

Remark 94. Notably, the rank does not change upon passing to a CM field extension E'/E (with suitably defined CM type Φ' extending Φ) because $\mathrm{T}_{\Phi'}$ will simply become $\mathrm{T}_{\Phi} \circ \mathrm{T}_{E'/E}$, and field traces of number fields are surjective.

For example, one can pass to the Galois closure. Thus, in the event where $E/\mathbb{Q}$ is Galois with $G \coloneqq \mathrm{Gal}(E/\mathbb{Q})$, we note that the existence of a normal basis implies that

$$\mathrm{rank}(E, \Phi) = \dim_{\mathbb{Q}} \mathbb{Q}[G]\Phi,$$

where we view Φ as an element of $\mathbb{Z}[G]$ given by the sum of its elements. Similarly, one can go down to $\mathrm{rank}_{\mathbb{Z}} \mathbb{Z}[G]\Phi$ and even multiply by Φ on either side.

The point of this definition is Proposition 89.

Proposition 95. Fix an abelian variety A with CM type (E, Φ). Then

$$\mathrm{rank}\, \mathrm{MT}(A) = \mathrm{rank}(E, \Phi).$$

Proof. By Proposition 89, we see that $\mathrm{rank}\, \mathrm{MT}(A)$ is the rank of the lattice spanned by

$$\sum_{\varphi \in \Phi} (\sigma\varphi)^{\vee}$$

as σ varies over $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Now, one can check that the rank of this lattice does not change if we pass from E to a Galois closure, so we assume that $E/\mathbb{Q}$ is Galois with Galois group G. Then we see that the above element is simply $\sigma\Phi$ for $\sigma \in G$, so we are indeed looking at the lattice $\mathbb{Z}[G]\Phi$, whose rank is simply the $\mathbb{Q}$-dimension of $\mathbb{Q}[G]\Phi$. Thus, we are done by Remark 94. ∎

Thus, we are motivated to understand ranks of these CM types. In the abelian case, one has the following character-theoretic result.

Lemma 96. Let (E, Φ) be a CM type such that $E/\mathbb{Q}$ is an abelian extension with Galois group G. Then $\mathrm{rank}(E, \Phi)$ equals the number of characters $\chi \colon G \to \mathbb{C}^{\times}$ such that

$$\chi(\Phi) \coloneqq \sum_{\varphi \in \Phi} \chi(\varphi)$$

is nonzero.

Proof. We will compute $\mathrm{rank}(E, \Phi)$ as $\dim_{\mathbb{C}} \mathbb{C}[G]\Phi$. One can diagonalize the G-action on $\mathbb{C}[G]$ into

$$\mathbb{C}[G] \cong \bigoplus_{\chi} \mathbb{C}_{\chi},$$

where G acts on $\mathbb{C}_{\chi}$ by χ. Thus, $\mathbb{Q}[G]\Phi$ will equal the sum of the spaces $\mathbb{C}_{\chi}\Phi$, but $\mathbb{C}_{\chi}\Phi$ is nonzero if and only if $\chi(\Phi) \neq 0$. ∎

Remark 97. Work in the setting of Lemma 96. Let $\iota \in G$ denote complex conjugation. If χ is a nontrivial character satisfying $\chi(\iota) = 1$, then we see that

$$0 = \sum_{g \in G} \chi(g) = \chi(\Phi + \iota\Phi) = 2\chi(\Phi),$$

so $\chi(\Phi) = 0$.

We are now ready to generalize Example 90.

Theorem 98. Fix a prime p, and consider the Jacobian A of the curve $C\colon y^p = x(x-1)$. Then

$$\operatorname{rank} \mathrm{MT}(A) = p+1.$$

In particular, equality holds in Proposition 84.

Proof. Recall from Example 88 that A is CM by $\mathbb{Q}(\zeta_p)$ with CM type $\Phi \coloneqq \{\varphi_1, \dots, \varphi_{(p-1)/2}\}$, where $\varphi_r \in \operatorname{Hom}(\mathbb{Q}(\zeta_p), \mathbb{C})$ sends $\varphi_r(\zeta_p) \coloneqq \zeta_p^r$.

We will use Lemma 96 for this computation. Let G be the Galois group $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, and we want to show that there are $p+1$ characters such that $\chi(\Phi) \neq 0$. Well, Remark 97 rules out nontrivial characters χ with $\chi(-1) = 1$, so we are left trying to show that all χ with $\chi(-1) = -1$ have $\chi(\Phi) \neq 0$.

This will use some algebraic number theory. For brevity, set $g \coloneqq \frac{p-1}{2}$. The key input is to use the class number formula for cyclotomic fields. Indeed, by using some form of the class number formula for $\mathbb{Q}(\zeta_p)$, we will show that

$$A \coloneqq \sum_{i=1}^{p-1} i\chi(i)$$

is nonzero for any nontrivial character χ. To see this, we begin by defining

$$L(s,\chi) \coloneqq \sum_{n=0}^{\infty} \frac{\chi(n)}{n^s}.$$

A computation with some contour integration shows that $L(s,\chi)$ analytically continues to $\mathbb{C}$ provided that χ is nontrivial (otherwise, there is a simple pole at $s=1$). Further, one can compute that

$$L(0,\chi) = -\frac{1}{p}\sum_{i=1}^{p-1} i\chi(i),$$

so we would like to show that $L(0,\chi)$ is nonzero. On the other hand, $L(0,\chi)$ is nonzero because

$$\zeta_K(s) = \prod_{\chi'} L(s,\chi'),$$

where the product is taken over Dirichlet characters $\chi' \pmod p$, and ζ_K only has a simple pole at $s=0$ explained by the trivial character and no other zeroes or poles.

We will transform this nonvanishing result into the required one. We begin by defining the family of sums

$$\begin{aligned}
A_< &\coloneqq \sum_{i=1}^{g} i\chi(i), \\
A_> &\coloneqq \sum_{i=g+1}^{p-1} i\chi(i), \\
A_0 &\coloneqq \sum_{i=1}^{g} 2i\chi(2i), \\
A_1 &\coloneqq \sum_{i=1}^{g} (2i-1)\chi(2i-1), \\
B_< &\coloneqq \sum_{i=1}^{g} \chi(i), \\
B_1 &\coloneqq \sum_{i=1}^{g} \chi(2i-1).
\end{aligned}$$

To continue, we describe some relations between these sums.

- One has $A = A_< + A_> = A_0 + A_1$.
- Because $\chi(-1) = -1$, we can see that $A_> = A_< - pB_<$ by sending $i \mapsto (p-i)$ in the sum. Combining with the previous point, we see that $A = 2A_< - pB_<$.
- On the other hand, considering B_1, we send $i \mapsto (p-i)$ to make the terms even and then factor out a factor of 2 to show that $B_1 = -\chi(2)B_<$.
- Similarly, considering A_1, we send $i \mapsto (p-i)$ to make the terms even and then factor our a factor of 2 to show that $A_1 = 2\chi(2)A_< - p\chi(2)B_<$. Summing, we see $A = A_1 + A_2 = 4\chi(2)A_< - p\chi(2)B_<$.

In total, we are able to see that

$$4\chi(2)A_< - p\chi(2)B_< = A = 2\chi(2)A_< - p\chi(2)B_<$$

is a nonzero value. However, $B_< = 0$ combined with the equality of the left and right sides would require $A_< = 0$ and then $A = 0$, which is a contradiction, as required. ■

Remark 99. By extending the above argument and doing some rather intricate combinatorics, the following has recently been proven: suppose the curve $C\colon y^p = x^a(x-1)$ has a not a primitive cubic root of unity (which is equivalent to $\operatorname{Jac} C$ failing to be simple). Then $\dim \mathrm{MT}(\operatorname{Jac} C) < \frac{p+1}{2}$ if and only if the following conditions are met.

(a) The multiplicative orders $\operatorname{ord}\left(-a^2-a\right)$ and $\operatorname{ord}(a)$ are odd.

(b) The three-adic valuations satisfy the inequality $v_3\left(\operatorname{ord}\left(a^2+a\right)\right) < v_3(\operatorname{ord}(a))$.

In fact,

$$\dim \mathrm{MT}(\operatorname{Jac} C) = \frac{p-1}{2}\left(1 - \frac{2}{\operatorname{lcm}(\operatorname{ord}(-a^2-a), \operatorname{ord}(a))}\right).$$