We finish the semester with a discussion of abelian varieties over finite fields and the Honda-Tate theorem. This theorem gives a bijection between abelian varieties over finite fields and Weil polynomials. We give a rough outline of the proof and a discussion of what we can say about abelian varieties in terms of this bijection. For more details see [1]. The Honda-Tate theorem also provides the foundation for the database of abelian varieties in the LMFDB,[1] since it reduces their enumeration to the enumeration of Weil polynomials as in Problem Set 12.

38.1 The Honda-Tate theorem

Fix a finite field $k = \mathbb{F}_q$; all varieties in this lecture will be defined over k. Recall that an *isogeny* between two abelian varieties is a surjective map $\psi : A \to B$ with finite kernel. Given such a map, there is a *dual isogeny* $\hat{\psi} : B \to A$ with the property that $\psi \circ \hat{\psi} = [\deg(\psi)]_B$ and $\hat{\psi} \circ \psi = [\deg(\psi)]_A$. We say that A is *isogenous* to B if there is an isogeny $A \to B$. The existence of dual isogenies shows that this is an equivalence relation; the equivalence class containing A is called its *isogeny class*.

A central role in the proof of the Honda-Tate theorem is played by the *endomorphism ring* $\mathrm{End}_k(A)$ and the endomorphism algebra $E = \mathrm{End}_k^0(A) = \mathrm{End}_k(A) \otimes \mathbb{Q}$.[2] We will denote the Frobenius morphism as $\pi_A : A \to A$, and consider it as an element of $\mathrm{End}_k(A)$. In general the ring $\mathrm{End}_k(A)$ is not commutative, but π_A is central. We may thus consider the field $F = \mathbb{Q}(\pi_A)$ generated by π_A as a subring of E.

Definition 38.1. An abelian variety A is *simple* if the only abelian subvarieties $A' \subseteq A$ are $A' = 0$ and $A' = A$. It is *absolutely simple* (or *geometrically simple*) if the base change $A_{\bar{k}}$ to $\bar{k}$ is simple.

One can detect whether an abelian variety is simple using its endomorphism algebra. In order to describe the result, we need a bit of noncommutative algebra.

Definition 38.2. If F is a field, an F-algebra is a ring E equipped with a ring homomorphism $F \to E$. Such an algebra is *central* if $zx = xz$ for all $z \in F$ and $x \in E$. A *(two-sided) ideal* is an additive subgroup $I \subseteq E$ so that $\alpha x \in I$ and $x\alpha \in I$ for all $\alpha \in E$ and $x \in I$. An algebra is *simple* if its only two sided ideals are 0 and E. A *division algebra* is an algebra where every element has a multiplicative inverse.

Theorem 38.3 (Wedderburn's theorem)**.** *If E is a central simple F-algebra then there is an integer d and a central division F-algebra D so that $E \cong M_d(D)$.*

Using this theorem, we can define an equivalence relation on the set of central simple F-algebras: two algebras are *Brauer equivalent* if their corresponding division algebras are isomorphic. The set of central simple F-algebras has a natural group structure, since the tensor product over F of two central algebras is still central and simple. This product

[1] http://www.lmfdb.org/Variety/Abelian/Fq/

[2] One explanation for tensoring with $\mathbb{Q}$ is the following interpretation of isogeny classes. If you define a category whose objects are abelian varieties over k and where the morphisms from A to B are given by $\mathrm{Hom}_k(A, B) \otimes \mathbb{Q}$ then the isomorphism classes in this category will exactly correspond to the isogeny classes. The reason for this is that, after tensoring with $\mathbb{Q}$, multiplication by any integer n becomes an isomorphism.

descends to the set of Brauer equivalence classes; the *Brauer group* $\mathrm{Br}(F)$ is the resulting group. For example, the Brauer group of any algebraically closed field is trivial, and $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$: the identity is the Brauer class of $\mathbb{R}$ and the nontrivial class is represented by the quaternion algebra $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ with $i^2 = j^2 = k^2 = ijk = -1$. The dimension over F of a central simple F-algebra is always a square.

The computation of the Brauer groups for local and global fields is one of the core results of class field theory.[3] If $K/\mathbb{Q}_p$ is finite then $\mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$, and if F is a number field then there is a short exact sequence

$$0 \to \mathrm{Br}(F) \to \bigoplus_v \mathrm{Br}(F_v) \to \mathbb{Q}/\mathbb{Z} \to 0,$$

where we identify $\mathrm{Br}(\mathbb{R})$ with $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ and the map to $\mathbb{Q}/\mathbb{Z}$ is the sum of all the coordinates. If $[E] \in \mathrm{Br}(F)$ is the class of a central simple F-algebra E we write $\mathrm{inv}_v(E)$ for the image of $[E]$ in $\mathrm{Br}(F_v) \cong \mathbb{Q}/\mathbb{Z}$. We say that E is *split* at v if $\mathrm{inv}_v(E) = 0$, ie if $E \otimes_F F_v$ is a matrix algebra over F_v. If E is not split at v we say it *ramifies* at v. This is used primarily for quaternion algebras (central simple F-algebras of dimension 4) where specifying the set of ramified places (any finite set with even cardinality) is enough to describe the quaternion algebra up to isomorphism.

We can now state the Honda-Tate theorem. A *Weil q-number* is a root of a Weil polynomial (all of whose roots have absolute value $\sqrt{q}$; we say that two Weil numbers are *conjugate* if they have the same minimal polynomial.

Theorem 38.4. *Let $k = \mathbb{F}_q$, with $q = p^a$.*

1. *The map $A \mapsto \pi_A$ defines a bijection between the set of k-isogeny classes of simple abelian varieties over k and the set of Weil q-numbers up to conjugacy.*
2. *If A is simple then $\mathrm{End}_k^0(A)$ is a central division F-algebra, where $F = \mathbb{Q}(\pi_A)$.*
3. *The division algebra E splits at all finite places not dividing p, is ramified at every real place of F, and for any place v dividing p we have*
$$\mathrm{inv}_v(E) = \frac{v(\pi_A)}{v(q)} \cdot [F_v : \mathbb{Q}_p].$$
4. *We have*
$$2\dim(A) = [E : F]^{1/2} \cdot [F : \mathbb{Q}].$$
In particular, if $h(x)$ is the minimal polynomial of π_A then the characteristic polynomial of π_A on $H^1_{\acute{e}t}(A, \mathbb{Q}_\ell)$ is $h(x)^{\sqrt{[E:F]}}$.

38.2 Proof sketch

The fact that π_A is the root of a Weil q-polynomial follows from the Weil conjectures, since the Weil polynomial $P_1(T)$ is the characteristic polynomial of Frobenius. To see that the map $A \mapsto \pi_A$ is injective, suppose that B is another abelian variety with $\pi_A = \pi_B$ (up to conjugacy), both roots of an irreducible polynomial h. One can check that, since A and B are simple, the characteristic polynomial of Frobenius is a power of $h(x)$ in each case, and

[3] there is a cohomological interpretation in terms of the Galois cohomology groups that we defined in Lecture 36: for any field K there is an isomorphism $\mathrm{Br}(K) \cong H^2(\mathrm{Gal}(K^{sep}/K), (K^{sep})^\times)$

thus one characteristic polynomial divides the other. This implies that A is isogenous to an abelian subvariety of B (or vice versa). Since both are simple, this must be B itself.

Surjectivity is harder; say that a Weil q-number π is *effective* if it is in the image of the map $A \mapsto \pi_A$. The basic idea is to use the theory over the complex numbers to find a complex abelian variety with endomorphism algebra L, where L is a CM-field[4] so that $E \otimes_F L$ is a matrix algebra over L. One then checks that this descends to an abelian variety over a number field (or p-adic field) with good reduction and so that the reduction has Weil number π^N for some $N \in \mathbb{Z}$. One can then use the theory of Weil restriction of scalars[5] to show that, if π^N is effective then so is π.

The rest of the statements involve computations with the endomorphism algebra and the Tate algebra of A.

38.3 Using the Weil polynomial

Many properties of the abelian variety are invariant under isogeny and can be read off of the Weil polynomial. Let A be an abelian variety of dimension g over $\mathbb{F}_q$ and $f(x)$ the characteristic polynomial of the Frobenius endomorphism of A.

1. The decomposition of A as a direct sum of simple factors (up to isogeny) matches the factorization of $f(x)$ into irreducibles. The exponents can be a bit off, since when A is simple $f(x)$ will be the eth power of an irreducible Weil polynomial. Here $e = \sqrt{[E:F]}$ can be computed in terms of the least common denominator of $\frac{v(\pi_A)}{v(q)}[F_v : \mathbb{Q}_p]$ for places v over p (together with $1/2$ if F is real).

2. When m is relatively prime to q, the m-torsion subgroup $A[m]$ over $\bar{k}$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{2g}$. But when p divides m the size drops: $\#A[p]$ is a power p^b of p between 1 and p^g. The integer b can be read off of $f(x)$: it is the number of slope 0 components of the Newton polygon of $f(x)$.

3. The largest possible endomorphism algebra occurs when $F = \mathbb{Q}$ and $[E:F] = (2g)^2$. This occurs precisely when E is isogenous to a product of supersingular elliptic curves,[6] or if all slopes of the Newton polygon are $1/2$. At the opposite extreme, the coefficient of x^g in f will be relatively prime to p if and only if $\#A[p] = p^g$; in this case A is called *ordinary*. For elliptic curves these are the only two possibilities, but in higher dimension there are other intermediate Newton polygons.

4. The number of $\mathbb{F}_q$ points on A is $\#A(\mathbb{F}_q) = f(1)$.

5. If A is isogenous to the Jacobian of a genus g curve C then the point counts of C are determined using the zeta function (and are, in particular, an isogeny invariant). For some A this would yield a negative count, or a count where the number of points drops from $\mathbb{F}_q$ to $\mathbb{F}_{q^j}$ for some j; such A cannot possibly be the Jacobian of a curve. The converse does not hold. We have good methods for determining whether A is isogenous to a Jacobian in dimension 2, but not in higher dimension.

[4] a degree 2 totally imaginary extension of a totally real field

[5] If X is a scheme over some extension F'/F then the restriction of scalars $\mathrm{Res}_{F'/F} X$ is a scheme Y over F so that $Y(M) = X(M \otimes_K K')$ for any K-algebra M

[6] An elliptic curve over $\mathbb{F}_q$ is supersingular when its endomorphism algebra is a quaternion algebra, which happens exactly when $\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$

References

[1] Kirsten Eisenträger. *The theorem of Honda and Tate.* http://math.stanford.edu/~conrad/vigregroup/vigre04/hondatate.pdf