Splitting of Abelian varieties

V. Kumar Murty
University of Toronto

Workshop on Curves and Applications
University of Calgary
August 21, 2013

A simple question about polynomials

- Question: Given an irreducible polynomial $f(T) \in \mathbb{Z}[T]$, and a prime p, does it necessarily remain irreducible modulo p?
- Answer: Obviously not.
- For example,

$$T^2 + 1 \equiv (T+1)^2 \pmod{2}.$$

A simple question about polynomials

- But sometimes, it does remain irreducible. For example

$$T^2 + 1 \pmod 7$$

  is irreducible.
- Question: Given an irreducible polynomial $f(T) \in \mathbb{Z}[T]$, is there a prime p such that $f(T) \pmod p$ is irreducible?
- Answer: Not necessarily!

A not so simple question about polynomials

- Question: Given an irreducible polynomial $f(T) \in \mathbb{Z}[T]$, is there a prime p such that $f(T) \pmod{p}$ is irreducible?
- Answer: No. A simple example is

$$f(T) = T^4 + 1.$$

- Another simple example is

$$f(T) = T^4 - 2T^2 + 9.$$

Factorization of $T^4 + 1 \pmod p$

- $T^4 + 1 = (T + 1)^4 \pmod 2$
- $T^4 + 1 = (T^2 + T - 1)(T^2 - T - 1) \pmod 3$
- $T^4 + 1 = (T^2 - 2)(T^2 + 2) \pmod 5$
- $T^4 + 1 = (T^2 + 3T + 1)(T^2 - 3T + 1) \pmod 7$

Factorization of $T^4 + 1 \pmod p$

- If $p \equiv 1 \pmod 4$, there is an a such that $a^2 \equiv -1 \pmod p$.
- With this a, we have

$$T^4 + 1 \;=\; (T^2 + a)(T^2 - a) \pmod p.$$

Factorization of $T^4 + 1 \pmod{p}$

- If $p \equiv 7 \pmod{8}$, there is a b such that $b^2 \equiv 2 \pmod{p}$.
- With this b, we have

$$T^4 + 1 = (T^2 + 1)^2 - 2T^2$$

$$= (T^2 - bT + 1)(T^2 + bT + 1) \pmod{p}.$$

- If $p \equiv 3 \pmod{8}$, there is a c such that $c^2 \equiv -2 \pmod{p}$ and

$$T^4 + 1 = (T^2 - cT - 1)(T^2 + cT - 1) \pmod{p}.$$

Another example

- Similarly, we see that

$$f(T) = T^4 - 2T^2 + 9$$

  is irreducible,

- but

$$f(T) \equiv (T+1)^4 \pmod 2$$

-

$$f(T) \equiv T^2(T^2-2) \pmod 3$$

-

$$f(T) \equiv (T^2+T+2)(T^2-T+2) \pmod 5, \cdots$$

Failure of a local-global principle

- Expressed another way, this means that an irreducible polynomial $f(T) \in \mathbb{Z}[T]$ may become *reducible* $\pmod{p}$ for *every* prime p.
- This is a failure of a local-global principle: reducibility locally everywhere does not imply global reducibility.

Failure of a local-global principle

- On the other hand, there are limits to this failure.
- If there is a prime p such that $f(T) \pmod{p}$ is irreducible, are there infinitely many such primes?
- Answer: Yes, in fact a positive density of primes. We shall see why later.

What is behind this?

- The answer comes from algebraic number theory.
- Let f be a normal polynomial and let E be the splitting field of f. Let $\mathcal{O}$ be the ring of integers.
- Dedekind's theorem: For all but finitely many p, the factorization of $f \pmod{p}$ is identical to the splitting of the ideal $p\mathcal{O}$ in the Dedekind domain $\mathcal{O}$.
- In other words,

$$f(T) = f_1(T)^{e_1} \cdots f_r(T)^{e_r} \pmod{p}$$

$$p\mathcal{O} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

An example

- Let R denote the ring $\mathbb{Z}[\sqrt{-1}]$.
- The factorization

$$T^2 + 1 \equiv (T + 1)^2 \pmod 2$$

corresponds to the factorization

$$2R = I^2$$

where $I = ((1 + \sqrt{-1})R)^2$.
- The irreducibility of

$$T^2 + 1 \pmod 7$$

means that $7R$ is a prime ideal in R.

The Frobenius automorphism

- We have

$$f(T) \; = \; f_1(T)^{e_1} \cdots f_r(T)^{e_r} \pmod{p}$$

$$p\mathcal{O} \; = \; \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

- To each $\mathfrak{p} = \mathfrak{p}_i$, there is an automorphism $\mathrm{Frob}_{\mathfrak{p}}$ in the Galois group of $E/\mathbb{Q}$.
- For most primes $\mathfrak{p}$, this is the unique automorphism σ which satisfies

$$\sigma(x) \; \equiv \; x^p \pmod{\mathfrak{p}}.$$

The Frobenius automorphism

- This automorphism $\mathrm{Frob}_{\mathfrak{p}}$ is an element which is of order equal to $\deg f_i$.
- In particular, if f is irreducible $\pmod{p}$, then $p\mathcal{O}$ stays prime in E and the order of $\mathrm{Frob}_{\mathfrak{p}}$ is $n = \deg f$.
- Thus, $\mathrm{Frob}_{\mathfrak{p}}$ generates $\mathrm{Gal}(E/\mathbb{Q})$ and so, this group must be cyclic.

The examples revisited

- In particular, consider again the examples given earlier

$$T^4 - 2T^2 + 9$$

and

$$T^4 + 1$$

- They have splitting field

$$\mathbb{Q}(\sqrt{-1}, \sqrt{2}) \text{ and } \mathbb{Q}(\zeta_8)$$

(respectively).

- Both have Galois group

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

A converse

- Conversely, suppose that f is normal and generates a cyclic extension.
- Then there are a positive density of primes p such that $f \pmod{p}$ is irreducible.
- This follows from the Chebotarev density theorem.

The general case

- What about non-normal polynomials? Consider the general case: the Galois group of f is the symmetric group S_n where $n = \deg\ f$.
- Then $f \pmod p$ factors according to the cycle structure of the conjugacy class of Frobenius automorphisms over p.
- In particular, $f \pmod p$ will be irreducible whenever the Frob_p is an n-cycle.
- To find such a prime, we need only check $p \ll\ (\log d_f)^2$ (if we believe the Generalized Riemann Hypothesis).

A geometric analogue

- We now ask for a geometric analogue of this question. A natural place to start is in the setting of Abelian varieties.
- Examples: elliptic curves (dimension 1), Jacobian of a curve of genus g (dimension g), and many more.
- Complete reducibility: any Abelian variety is isogenous to a product of simple (absolutely simple) Abelian varieties and this factorization is essentially unique.

The Geometric Question

- Given a simple or absolutely simple Abelian variety over a number field, is there a prime (infinitely many primes, a positive density of primes ...) for which the reduction A_p modulo p is simple or absolutely simple?
- Answer: No.
- The situation depends on the endomorphism algebra of A.

The endomorphism algebra

- The set of morphisms of algebraic varieties

$$A \longrightarrow A$$

that are also group homomorphisms form (after tensoring with $\mathbb{Q}$) a $\mathbb{Q}$ algebra

$$\mathrm{End}(A) \otimes \mathbb{Q}.$$

- The Abelian variety A is simple if and only if this algebra is a division algebra.

Abelian surfaces with quaternionic multiplication

- Let A be an Abelian surface with multiplication by an indefinite quaternion division algebra over $\mathbb{Q}$.
- There are such Abelian surfaces defined over a number field and that are absolutely simple.
- But at any prime v of good reduction,

$$A_v \sim E_v^2$$

where E_v is an elliptic curve.

What is behind this?

- Reduction modulo v induces an injection of $\mathbb{Q}$-algebras
$$\mathrm{End}(A) \otimes \mathbb{Q} \longrightarrow \mathrm{End}(A_v) \otimes \mathbb{Q}.$$
- The endomorphism algebra of an absolutely simple Abelian surface over a finite field is commutative.
- The second assertion follows from a theorem of Tate (If the endomorphism algebra is non-commutative, it is an indefinite quaternion division algebra over $\mathbb{Q}$, and hence of degree 4 over $\mathbb{Q}$. Tate's theorem implies that it must be commutative. Contradiction.)

Failure of a local-global principle

- This phenomenon is a failure of the local-global principle.
- Local-global problems are usually studied in the context of Diophantine equations.
- A classical example where the principle holds is the Hasse-Minkowski Theorem:
- For F a quadratic form, a p-adic solution of $F = 0$ for every p (including "infinity") implies the existence of a rational solution.

Failure of a local-global principle

- In many other contexts, it fails, for example for cubic and quartic curves.
- It even fails for binary quadratic forms if we ask for *integral* rather than rational solutions.
- The degree of failure can sometimes be measured by a group (eg. Genus theory, Shafarevitch-Tate group, Brauer group, etc.)
- There should be a Brauer group-theoretic way of describing the obstruction.

Failure of a local-global principle

- In our case, the failure has to do with the non-existence of primes v for which the Frobenius torus is irreducible and of maximal dimension.
- The Galois group attached to the Abelian variety plays a role.

Digression: L-functions

- This means that the L-function of such an A has an Euler product in which each factor is a square:

$$L(A, s) = \prod_v L(E_v, s)^2.$$

- Nevertheless, its 'square root' is not expected to have good properties. (We can probably prove this.)
- Note that the $\{E_v\}$ do not lift to an elliptic curve E over a number field. (If they did, we can show that A is isogenous to $E \times E$.)

Digression: Lifting Elliptic Curves

- For each $x \geq 1$, let E_x denote the lift of all E_v (for $Nv \leq x$) of minimal conductor $f(x)$ (say).
- If there were a lift of all the E_v then $f(x)$ would be constant

Theorem (joint work with Sanoli Gun)

Assume the GRH. If

$$f(x) \ll \exp\{x^{1/2-\epsilon}\}$$

then in fact $f(x)$ is constant and the E_v can be lifted.

Idea of Proof

- If E_1 and E_2 are non-isogenous curves over $\mathbb{Q}$, there exists a prime
$$q \ll (\log \max\{f(E_1), f(E_2)\})^2$$
for which $a_q(E_1) \neq a_q(E_2)$.
- Let M and N be such that $M < N \leq 2M$. If E_N is not isogenous to E_M, then $a_q(E_N) \neq a_q(E_M)$ for some $q \ll \ N^{1-\epsilon}$. But by definition, $q \geq N$. Contradiction.

The endomorphism algebra

- There is a lot of work on the endomorphism algebras of Abelian varieties, and in particular on which division algebras can occur.
- The first constraint comes from the fact that $\mathrm{End}(A) \otimes \mathbb{Q}$ also acts on the cohomology of A, and in particular on $H^1(A)$.

The cohomology of A

- Over the complex numbers,

$$A(\mathbb{C}) = \mathbb{C}^d / L$$

  where L is a lattice (i.e. $L \simeq \mathbb{Z}^{2d}$).
- In this case,

$$H^1(A) = L \otimes \mathbb{Q}.$$

- In general, we have to define it much more abstractly.

Endomorphisms and cohomology

- We see therefore that there is a map

$$\mathrm{End}(A) \otimes \mathbb{Q} \longrightarrow \mathrm{End}(H^1(A)).$$

- This map is *injective*.
- Therefore, $\mathrm{End}(A) \otimes \mathbb{Q}$ can be embedded into the matrix algebra $M_{2d}(\mathbb{Q})$.
- In particular, the maximal commutative semisimple subalgebra of $\mathrm{End}(A) \otimes \mathbb{Q}$ is of degree $\leq 2d$.

Abelian varieties of CM-type

- If this maximum dimension is attained, we say that A has *complex multiplication* or is of *CM*-type.

Theorem (joint work with Patankar)

Let A be a simple Abelian variety of CM-type and let K be a number field so that A and its endomorphisms are defined over K. Then, for a set of primes v of K of density 1, A_v is simple.

The Galois group of an Abelian variety

- The Galois group is defined in terms of points of finite order.
- Suppose that A is d-dimensional and defined over K. Then, the equation
$$nP = \mathcal{O}$$
will have n^{2d} solutions $P \in A(\overline{K})$.
- The collection of these solutions $A[n]$ forms a finite Abelian group
$$A[n] \ \simeq \ (\mathbb{Z}/n\mathbb{Z})^{2d}$$
on which $\mathrm{Gal}(\overline{K}/K)$ acts.

The Galois group of an Abelian variety

- Fix a prime ℓ and consider the Galois modules $A[\ell^m]$ as m varies.
- They form an inverse system under multiplication by ℓ.
- In other words, for $m_2 \geq m_1$, we have

$$\ell^{m_2 - m_1} : \ A[\ell^{m_2}] \ \longrightarrow \ A[\ell^{m_1}].$$

- We consider the inverse limit $T_\ell(A)$ as $\mathrm{Gal}(\overline{K}/K)$-module.

The Galois group of an Abelian variety

- As Abelian group
$$T_\ell(A) \simeq \mathbb{Z}_\ell^{2d}.$$
- There is a symplectic form which is respected by the Galois action
- The image of
$$\rho_{A,\ell} : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(T_\ell(A))$$
lies in $GSp_{2d}(\mathbb{Z}_\ell)$.

The Galois group of an Abelian variety

- The image of $\rho_{A,\ell}$ is called the ℓ-adic Galois group of A.
- Conjecturally, it is "independent of ℓ".
- Generically, we expect that the Galois group is the full group of symplectic similitudes $GSp_{2d}(\mathbb{Z}_\ell)$.

The Galois group and the local-global problem

- Chai and Oort have shown that if the Galois group of an absolutely simple Abelian variety defined over a number field is the full group of symplectic similitudes, then there are a positive density of primes at which the reduction is also absolutely simple.
- The *CM*-case is the other extreme: the Galois group is as "small" as possible. We have shown that a similar result (even stronger) holds in this case.
- How do we bridge these two cases?

The endomorphism algebra

- For a "generic" Abelian variety

$$\mathrm{End}_{\overline{K}}(A) \; = \; \mathbb{Z}.$$

- For an absolutely simple *CM*- Abelian variety

$$\mathrm{End}_{\overline{K}}(A) \text{ is a commutative field.}$$

- In both cases, the reduction stays simple for a set of primes of positive density.
- For absolutely simple Abelian surfaces with quaternionic endomorphism algebra, their reduction modulo every prime is *not* simple.

A conjecture

Conjecture (joint work with Patankar)

Let A be defined over K and absolutely simple. Suppose that K is sufficiently large. There exists a set of primes v of K of density one for which the reduction A_v is absolutely simple if and only if $\mathrm{End}(A)$ is commutative.

Necessity

- A special case of a theorem of Tate asserts that if A_p defined over $\mathbb{F}_p$ is simple, then $\mathrm{End}(A_p)$ is commutative.
- On the other hand, if A is defined over O_K, the map

$$\mathrm{End}(A) \longrightarrow \mathrm{End}(A_v)$$

is injective.
- Hence, if there exists a set of primes v of density 1 at which A_v remains absolutely simple, then this set has to contain primes of degree 1 and then by the above remark, $\mathrm{End}(A_v)$, and hence also $\mathrm{End}(A)$ is commutative.

Known cases of the conjecture

- Abelian varieties associated to elliptic modular forms (joint work with Patankar)
- A having no endomorphisms and maximum monodromy (Chai-Oort)
- $\mathrm{End}(A) \otimes \mathbb{Q}$ is a definite quaternion algebra over a totally real field F and $\dim X/2[F : \mathbb{Q}]$ is odd (Achter)
- A satisfying the Mumford-Tate conjecture (Zywina)

The monodromy representation

- We have
$$\mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}(H^1_\ell(\overline{A})).$$
- Denote by k_v the residue field at v. If v is a prime of good reduction, then by Néron-Ogg-Shafarevich, the monodromy representation is unramified at v (that is, the inertia group at v acts trivially).
- Thus, the action of the decomposition group can be identified with the action of $\mathrm{Gal}(\overline{k_v}/k_v)$.
- We have
$$H^1_\ell(\overline{A}) \simeq H^1_\ell(\overline{A_v})$$
as modules for $\mathrm{Gal}(\overline{k_v}/k_v)$.

The image

- Denote by M_ℓ the image of the monodromy representation.
- Denote by M_ℓ^{Zar} its Zariski closure in $\mathrm{GL}(H_\ell^1(\overline{A}))$. If we assume that K is sufficiently large, this group is connected.
- The Mumford-Tate conjecture asserts that this group is $MT(A)(\mathbb{Q}_\ell)$.
- It is known that $M_\ell \subseteq MT(A)(\mathbb{Q}_\ell)$ (Deligne).

Consequences of Tate's theorem

- Tate's theorem tells us that for any prime ℓ unequal to the characteristic of the residue field k_v, we have

$$\mathrm{End}(A_v) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \;\simeq\; \mathrm{End}_{F_v}(H^1_\ell(\overline{A_v})).$$

- Hence, if F_v acts irreducibly on $H^1_\ell(\overline{A_v})$, then A_v is simple.
- Equivalently if F_v acts irreducibly on $H^1_\ell(\overline{A})$, then A_v is simple.
- This condition is not necessary: A_v may be simple but $\mathrm{End}(A_v) \otimes \mathbb{Q}_\ell$ may not be a simple algebra.

Consequences of the Chebotarev Density Theorem

- The subset X_ℓ of M_ℓ consisting of elements which act irreducibly on $H^1_\ell(\overline{A})$ is a union of conjugacy class and is open in M_ℓ.
- Its measure is the Dirichlet density of the set

$$\{v : F_v \in X_\ell\}.$$

- By openness, if it is nonempty, it has positive measure.
- It is contained in the set

$$\{v : A_v \text{ is simple }\}.$$

Maximal tori of M_ℓ^{Zar}

- Any element of X_ℓ lies in a maximal torus that acts irreducibly on $H^1_\ell(\overline{A})$.
- Conversely, any torus of M_ℓ^{Zar} that acts irreducibly on $H^1_\ell(\overline{A})$ contains an open dense subset all of whose $\mathbb{Q}_\ell$ points act irreducibly. Hence, X_ℓ is nonempty.
- Thus, we are looking for maximal tori of M_ℓ^{Zar} that act irreducibly.

An important restriction

- By Tate's theorem, if $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ is not a field, M_ℓ^{Zar} acts reducibly.
- Hence, we assume that A is such that $\mathrm{End}(A) \otimes \mathbb{Q}$ is a commutative field and that there exists a prime ℓ for which $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$ is a field.
- Also, we may replace M_ℓ^{Zar} with its derived subgroup $G = [M_\ell^{\mathrm{Zar}}, M_\ell^{\mathrm{Zar}}]$.

The reformulated question

- Let G be a semisimple algebraic group over an extension E of $\mathbb{Q}_\ell$ and

$$\rho_V : G \longrightarrow \mathrm{GL}(V)$$

an absolutely irreducible representation with finite kernel. Under what conditions can we assert that some maximal torus of G acts irreducibly on V?

Roots and Weights

- Let F be a Galois extension of E over which there is a split maximal torus T. Let B be a Borel subgroup containing T.
- Let $X = \mathrm{Hom}(T, \mathbb{G}_{m/F})$ and $Y = \mathrm{Hom}(\mathbb{G}_{m/F}, T)$. Both are modules for $\Gamma = \mathrm{Gal}(F/E)$.
- The set $\Omega(V)$ of *weights* of V is the subset of characters in X which appear in the action of T on V.
- The weights and multiplicities determine the representation V up to isomorphism.
- Since ρ_V has finite kernel, the set of weights $\Omega(V)$ spans the $\mathbb{Q}$-vector space $X \otimes \mathbb{Q}$.

Minuscule Weights

- There is an action of Γ as well as the Weyl group W on the set of weights $\Omega(V)$.
- V is a minuscule representation if W acts transitively on the weights $\Omega(V)$.
- If a maximal torus T of G acts irreducibly on V then V is minuscule.

Classificiation

Theorem (joint work with Ying Zong)

There exists a maximal torus of G that acts irreducibly on V if and only if V is minuscule and any simple factor of G and its associated highest weight is one of the following:

- (A_n, α_1) *and* (A_n, α_n)
- (A_{ℓ^d-1}, α_2) *and* $(A_{\ell^d-1}, \alpha_{\ell^d-2})$ *for* $d \geq 1$
- (C_n, α_1) *for* $n \geq 2$
- (D_n, α_1) *for* n *even and* ≥ 4
- $({}^2D_n, \alpha_1)$
- *Another 20 possibilities which are either residue characteristic dependent or are isolated.*

Tate Cycles

- So far, we have been discussing divisors.
- Tate's general conjecture asks about cycles of any codimension.
- The Tate ring $Ta_\ell(A)$ is the collection of all cohomology classes that are fixed (after twist) by an open subgroup of the Galois group.
- Tate's conjecture is that these classes are all algebraic.
- Tate, Faltings, Zarhin: proved the case of divisors.

Tate Cycles

- Reduction modulo v induces an injection of Tate cycles $Ta_\ell(A)$ on A into the space of Tate cycles $Ta_\ell(A_v)$ on A_v.
- For an Abelian variety to split when reduced modulo v may be seen as the reduction A_v acquiring an extra Tate cycle.
- We might ask for a criterion by which $Ta_\ell(A) \simeq Ta_\ell(A_v)$ for a set of primes of positive density or even density 1.

The case of CM Abelian Varieties

Theorem (joint work with Patankar)

Let A be of CM-type and assume that K is sufficiently large so that A and all its endomorphisms are defined over K. Then for a set of primes v of K of density 1, we have

$$Ta_\ell(A) \;\simeq\; Ta_\ell(A_v).$$

In particular, the Tate conjecture for A implies the Tate conjecture for almost all A_v.