A Torelli theorem over finite fields

November 2008

Divisibilities

Homework

Let a, b be integers ≥ 2. Assume that

$$a^n - 1 \mid b^n - 1,$$

for all $n \in \mathbb{N}$. Then b is a power of a.

Divisibilities

Homework

Let a, b be integers ≥ 2. Assume that

$$a^n - 1 \mid b^n - 1,$$

for all $n \in \mathbb{N}$. Then b is a power of a.

Bugeaud, Corvaja, Zannier (2003)

Let $a, b \in \mathbb{N}$ be multiplicatively independent. Fix $\epsilon > 0$. Then there exists a $c = c(a, b, \epsilon)$ such that

$$\log(\gcd(a^n - 1, b^n - 1)) \leq \epsilon n + c,$$

for all $n \in \mathbb{N}$.

Divisibility

Let K be a number field. For $\alpha, \beta \in K^*$, put

$$v^+(\alpha) := \max\{0, v(\alpha)\}$$

$$h_{\text{gcd}}(\alpha - 1, \beta - 1) := \sum_v \min\{v^+(\alpha - 1), v^+(\beta - 1)\}.$$

Corvaja-Zannier (2005)

Let S be a finite set of places of K and $\alpha, \beta \in \mathcal{O}_S$. Then

$$h_{\text{gcd}}(\alpha - 1, \beta - 1) \leq \epsilon \max\{h(\alpha), h(\beta)\} + c(K, S, \epsilon).$$

Vojta's conjecture

- K number field, S finite set of places
- X/K smooth, $D \subset X$ normal crossings
- L very ample divisor on X

Conjecture

For all $P \in X(K) \setminus Z_\epsilon$ one has

$$h_{D,S}(P) + h_{K_X}(P) \leq \epsilon h_L(P).$$

Vojta's conjecture

Silverman (2004)

Let $\pi : \tilde{X} = \mathrm{Bl}_Y(X) \to X = \mathbb{P}^1 \times \mathbb{P}^1$, with $Y = (1,1)$, and let E be the exceptional divisor. Then

$$h_{\mathrm{gcd}}(\alpha - 1, \beta - 1) = h_{\tilde{X},E}((\alpha, \beta)) + O(1),$$

for all $\alpha, \beta \in \bar{\mathbb{Q}}, \neq (1,1)$.

Vojta's conjecture

Silverman (2004)

Let $\pi : \tilde{X} = \mathrm{Bl}_Y(X) \to X = \mathbb{P}^1 \times \mathbb{P}^1$, with $Y = (1,1)$, and let E be the exceptional divisor. Then

$$h_{\mathrm{gcd}}(\alpha - 1, \beta - 1) = h_{\tilde{X},E}((\alpha, \beta)) + O(1),$$

for all $\alpha, \beta \in \bar{\mathbb{Q}}, \neq (1,1)$. When $\alpha, \beta \in \mathcal{O}_S$ are multiplicatively independent, Vojta's conjecture implies the theorem of Corvaja-Zannier.

Vojta's conjecture

Silverman (2004)

Let $\pi : \tilde{X} = \mathrm{Bl}_Y(X) \to X = \mathbb{P}^1 \times \mathbb{P}^1$, with $Y = (1,1)$, and let E be the exceptional divisor. Then

$$h_{\mathrm{gcd}}(\alpha - 1, \beta - 1) = h_{\tilde{X},E}((\alpha, \beta)) + O(1),$$

for all $\alpha, \beta \in \bar{\mathbb{Q}}, \neq (1,1)$. When $\alpha, \beta \in \mathcal{O}_S$ are multiplicatively independent, Vojta's conjecture implies the theorem of Corvaja-Zannier.

This instance of Vojta's conjecture (on $\mathbb{G}_m \times \mathbb{G}_m \subset \mathbb{P}^1 \times \mathbb{P}^1$) is proved using Schmidt's subspace theorem.

Recurrence sequences

$R : \mathbb{N} \to \mathbb{C}$ is a linear recurrence if

$$R(n+r) = \sum_{i=0}^{r-1} a_i R(n+i),$$

for some $a_i \in \mathbb{C}$ and all $n \in \mathbb{N}$.

Recurrence sequences

$R : \mathbb{N} \to \mathbb{C}$ is a linear recurrence if

$$R(n+r) = \sum_{i=0}^{r-1} a_i R(n+i),$$

for some $a_i \in \mathbb{C}$ and all $n \in \mathbb{N}$. Equivalently,

$$R(n) = \sum_{\gamma \in \Gamma^0} c_\gamma(n)\gamma^n,$$

where

- $c_\gamma \in \mathbb{C}[x]$
- $\Gamma^0 \subset \mathbb{C}^*$ is a finite set of roots of R.

Recurrence sequences

$R : \mathbb{N} \to \mathbb{C}$ is a linear recurrence if

$$R(n+r) = \sum_{i=0}^{r-1} a_i R(n+i),$$

for some $a_i \in \mathbb{C}$ and all $n \in \mathbb{N}$. Equivalently,

$$R(n) = \sum_{\gamma \in \Gamma^0} c_\gamma(n) \gamma^n,$$

where

- $c_\gamma \in \mathbb{C}[x]$
- $\Gamma^0 \subset \mathbb{C}^*$ is a finite set of roots of R.

R is called simple if $c_\gamma \in \mathbb{C}^*$, for all $\gamma \in \Gamma^0$.

Recurrence sequences

Let $\Gamma \subset \mathbb{C}^*$ be the group generated by Γ^0. Assume that Γ is torsion-free.

Recurrence sequences

Let $\Gamma \subset \mathbb{C}^*$ be the group generated by Γ^0. Assume that Γ is torsion-free.

- $\{\gamma_1, \ldots, \gamma_r\}$: a basis of Γ
- $\mathbb{C}[\Gamma]$: algebra of Laurent polynomials $x^\gamma = \prod_{j=1}^r x_j^{g_j}$, where

$$\gamma = \prod_{i=1}^r \gamma_i^{g_i} \in \Gamma.$$

Recurrence sequences

Let $\Gamma \subset \mathbb{C}^*$ be the group generated by Γ^0. Assume that Γ is torsion-free.

- $\{\gamma_1, \ldots, \gamma_r\}$: a basis of Γ
- $\mathbb{C}[\Gamma]$: algebra of Laurent polynomials $x^\gamma = \prod_{j=1}^r x_j^{g_j}$, where

$$\gamma = \prod_{i=1}^r \gamma_i^{g_i} \in \Gamma.$$

- $\mathfrak{R}_\Gamma$: ring of simple linear recurrences with roots in Γ.

Recurrence sequences

Fact

$\mathfrak{R}_\Gamma$ is isomorphic to $\mathbb{C}[\Gamma]$.

Recurrence sequences

Fact

$\mathfrak{R}_\Gamma$ is isomorphic to $\mathbb{C}[\Gamma]$.

$$R \mapsto F_R \in \mathbb{C}[\Gamma]$$

Recurrence sequences

Corvaja-Zannier, *Inv. Math.* (2002)

Let R and $\tilde{R}$ be simple linear recurrences such that

1. $R(n), \tilde{R}(\tilde{n}) \neq 0$, for all $n, \tilde{n} \gg 0$;
2. the subgroup $\Gamma \subset \mathbb{C}^*$ generated by the roots of R and $\tilde{R}$ is torsion-free;
3. there is a finitely-generated subring $\mathfrak{A} \subset \mathbb{C}$ with $R(n)/\tilde{R}(n) \in \mathfrak{A}$, for infinitely many $n \in \mathbb{N}$.

Recurrence sequences

Corvaja-Zannier, *Inv. Math.* (2002)

Let R and $\tilde{R}$ be simple linear recurrences such that

1. $R(n), \tilde{R}(\tilde{n}) \neq 0$, for all $n, \tilde{n} \gg 0$;
2. the subgroup $\Gamma \subset \mathbb{C}^*$ generated by the roots of R and $\tilde{R}$ is torsion-free;
3. there is a finitely-generated subring $\mathfrak{A} \subset \mathbb{C}$ with $R(n)/\tilde{R}(n) \in \mathfrak{A}$, for infinitely many $n \in \mathbb{N}$.

Then

$$\begin{array}{rcl} Q : \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & R(n)/\tilde{R}(n) \end{array}$$

is a simple linear recurrence. In particular, the $F_Q \in \mathbb{C}[\Gamma]$ and

$$F_Q \cdot F_{\tilde{R}} = F_R.$$

Laurent polynomials

Lemma

Let $\Gamma \subset \mathbb{C}^*$ be finitely-generated and torsion-free. Let $\mathbb{C}[\Gamma]$ be the ring of Laurent polynomials.

- If $\gamma \in \Gamma$ is primitive then $x^\gamma - \lambda$ is irreducible in $\mathbb{C}[\Gamma]$.

Laurent polynomials

Lemma

Let $\Gamma \subset \mathbb{C}^*$ be finitely-generated and torsion-free. Let $\mathbb{C}[\Gamma]$ be the ring of Laurent polynomials.

- If $\gamma \in \Gamma$ is primitive then $x^\gamma - \lambda$ is irreducible in $\mathbb{C}[\Gamma]$.
- For $\gamma, \gamma' \in \Gamma$, the polynomials $x^\gamma - 1, x^{\gamma'} - 1$ are not coprime in $\mathbb{C}[\Gamma]$ if and only if γ, γ' generate a cyclic subgroup in Γ.

Recurrence sequences

- X: smooth projective variety over $\mathbb{F}_q$ of dimension d
- k_n/k: unique extension of degree n
- Fr: Frobenius on the étale cohomology $H^*_{et}(X, \mathbb{Q}_\ell)$, with $\ell \nmid q$
- $\Gamma^0 := \{\alpha_{ij}\}$: corresponding eigenvalues

Recurrence sequences

- X: smooth projective variety over $\mathbb{F}_q$ of dimension d
- k_n/k: unique extension of degree n
- Fr: Frobenius on the étale cohomology $H^*_{et}(X, \mathbb{Q}_\ell)$, with $\ell \nmid q$
- $\Gamma^0 := \{\alpha_{ij}\}$: corresponding eigenvalues

$$\#X(k_n) := \mathrm{tr}(\mathrm{Fr}^n) = \sum_{i=0}^{2d} (-1)^i c_{ij} \alpha_{ij}^n,$$

where $c_{ij} \in \mathbb{C}^*$.

Recurrence sequences

- X: smooth projective variety over $\mathbb{F}_q$ of dimension d
- k_n/k: unique extension of degree n
- Fr: Frobenius on the étale cohomology $H^*_{et}(X, \mathbb{Q}_\ell)$, with $\ell \nmid q$
- $\Gamma^0 := \{\alpha_{ij}\}$: corresponding eigenvalues

$$\#X(k_n) := \mathrm{tr}(\mathrm{Fr}^n) = \sum_{i=0}^{2d} (-1)^i c_{ij} \alpha_{ij}^n,$$

where $c_{ij} \in \mathbb{C}^*$. This is a simple linear recurrence.

Recurrence sequences

- X: smooth projective variety over $\mathbb{F}_q$ of dimension d
- k_n/k: unique extension of degree n
- Fr: Frobenius on the étale cohomology $H^*_{et}(X, \mathbb{Q}_\ell)$, with $\ell \nmid q$
- $\Gamma^0 := \{\alpha_{ij}\}$: corresponding eigenvalues

$$\#X(k_n) := \mathrm{tr}(\mathrm{Fr}^n) = \sum_{i=0}^{2d} (-1)^i c_{ij} \alpha_{ij}^n,$$

where $c_{ij} \in \mathbb{C}^*$. This is a simple linear recurrence. Let $\Gamma_X \subset \mathbb{C}^*$ be the multiplicative group generated by α_{ij}.

Recurrence sequences

Theorem

Let X and $\tilde{X}$ be smooth projective varieties over a finite field k_1, resp. $\tilde{k}_1$. Assume that

$$\#X(k_n) \mid \#\tilde{X}(\tilde{k}_n),$$

for infinitely many $n \in \mathbb{N}$. Then $\mathrm{char}(k_1) = \mathrm{char}(\tilde{k}_1)$ and

$$\Gamma_X \otimes \mathbb{Q} \subseteq \Gamma_{\tilde{X}} \otimes \mathbb{Q}.$$

Abelian varieties

Let A be an abelian variety over $k_1 := \mathbb{F}_q$. Let $\{\alpha_j\}_{j=1,\ldots,2g}$ be the set of eigenvalues of Frobenius on $H^1_{et}(A, \mathbb{Q}_\ell)$, for $\ell \neq p$. Let k_n/k_1 be the unique extension of degree n. The sequence

$$R(n) := \#A(k_n) = \prod_{j=1}^{2g} (\alpha_j^n - 1).$$

is a simple linear recurrence.

Abelian varieties

Let A be an abelian variety over $k_1 := \mathbb{F}_q$. Let $\{\alpha_j\}_{j=1,\dots,2\mathrm{g}}$ be the set of eigenvalues of Frobenius on $H^1_{et}(A, \mathbb{Q}_\ell)$, for $\ell \neq p$. Let k_n/k_1 be the unique extension of degree n. The sequence

$$R(n) := \#A(k_n) = \prod_{j=1}^{2\mathrm{g}} (\alpha_j^n - 1).$$

is a simple linear recurrence.

Theorem

Let A and $\tilde{A}$ be abelian varieties of dimension g over finite fields k_1, resp. $\tilde{k}_1$. Let R and $\tilde{R}$ be the corresponding recurrences. Assume that $\tilde{R(n)} \mid R(n)$, for infinitely many $n \in \mathbb{N}$. Then $\mathrm{char}(k_1) = \mathrm{char}(\tilde{k}_1)$ and A and $\tilde{A}$ are isogenous.

Sketch of proof

Assume that the group Γ generated by $\{\alpha_j\}$ is torsion-free. Fix a basis $\gamma_1, \ldots, \gamma_r$ of Γ and write

$$\alpha_j = \prod \gamma_j^{a_{ij}}.$$

Sketch of proof

Assume that the group Γ generated by $\{\alpha_j\}$ is torsion-free. Fix a basis $\gamma_1, \ldots, \gamma_r$ of Γ and write

$$\alpha_j = \prod \gamma_j^{a_{ij}}.$$

Since all conjugates of α_j have absolute value $\sqrt{q}$, we have

- either $\alpha_j = \alpha_{j'}$
- or $\alpha_j, \alpha_{j'}$ generate a subgroup of rank 2 in Γ.

Sketch of proof

Assume that the group Γ generated by $\{\alpha_j\}$ is torsion-free. Fix a basis $\gamma_1, \ldots, \gamma_r$ of Γ and write

$$\alpha_j = \prod \gamma_j^{a_{ij}}.$$

Since all conjugates of α_j have absolute value $\sqrt{q}$, we have

- either $\alpha_j = \alpha_{j'}$
- or $\alpha_j, \alpha_{j'}$ generate a subgroup of rank 2 in Γ.

Let $\{\alpha_j\} = \sqcup_{s=1}^{t} I_s$ be a subdivision into subsets of equal elements, $t \leq 2g$. Put $d_s := \# I_s$.

Sketch of proof

Let $\Gamma \subset \mathbb{C}^*$ be the group generated by $\{\alpha_j\}$ and $\{\tilde{\alpha}_j\}$. Again, we may assume that Γ is torsion free.
The Laurent polynomials for $R(n)$, $\tilde{R}(n)$ have the form:

$$F(x) := \prod_{s=1}^{t}(\prod_{i=1}^{r} x_i^{a_{is}} - 1)^{d_s}, \quad \tilde{F}(x) := \prod_{\tilde{s}=1}^{\tilde{t}}(\prod_{i=1}^{r} x_i^{\tilde{a}_{i\tilde{s}}} - 1)^{d_{\tilde{s}}}.$$

Lemma

$$\gcd(\prod_{i=1}^{r} x_i^{a_{is}} - 1, \prod_{i=1}^{r} x_i^{a_{is'}} - 1) = 1,$$

for $s \neq s'$.

Sketch of proof

Let $\Gamma \subset \mathbb{C}^*$ be the group generated by $\{\alpha_j\}$ and $\{\tilde{\alpha}_j\}$. Again, we may assume that Γ is torsion free.
The Laurent polynomials for $R(n)$, $\tilde{R}(n)$ have the form:

$$F(x) := \prod_{s=1}^{t}(\prod_{i=1}^{r} x_i^{a_{is}} - 1)^{d_s}, \quad \tilde{F}(x) := \prod_{\tilde{s}=1}^{\tilde{t}}(\prod_{i=1}^{r} x_i^{\tilde{a}_{i\tilde{s}}} - 1)^{d_{\tilde{s}}}.$$

Lemma

$$\gcd(\prod_{i=1}^{r} x_i^{a_{is}} - 1, \prod_{i=1}^{r} x_i^{a_{is'}} - 1) = 1,$$

for $s \neq s'$.

Same holds for $\tilde{F}$.

Sketch of proof

Using Lemma above, have $t = \tilde{t}$. Order indices so that $\#I_s = \#\tilde{I}_s$ and so that the multiplicative sugroups generated by $\alpha_s \in I_s$ and $\tilde{\alpha}_s \in \tilde{I}_s$ have rank 1, for all $s = 1, \ldots, t$.

Sketch of proof

Using Lemma above, have $t = \tilde{t}$. Order indices so that $\#I_s = \#\tilde{I}_s$ and so that the multiplicative sugroups generated by $\alpha_s \in I_s$ and $\tilde{\alpha}_s \in \tilde{I}_s$ have rank 1, for all $s = 1, \ldots, t$.

It follows that $\tilde{\alpha}_s = \alpha_s^u$, where $u \in \mathbb{Q}$ depends only on k_1 and $\tilde{k}_1$.

Sketch of proof

Using Lemma above, have $t = \tilde{t}$. Order indices so that $\# I_s = \# \tilde{I}_s$ and so that the multiplicative sugroups generated by $\alpha_s \in I_s$ and $\tilde{\alpha}_s \in \tilde{I}_s$ have rank 1, for all $s = 1, \dots, t$.

It follows that $\tilde{\alpha}_s = \alpha_s^u$, where $u \in \mathbb{Q}$ depends only on k_1 and $\tilde{k}_1$. Thus some powers of the Frobenius morphisms $\mathrm{Fr}, \tilde{\mathrm{Fr}}$ have the same sets of eigenvalues with equal multiplicities.

A theorem of Tate

$$\mathrm{Hom}(A, \tilde{A}) \otimes \mathbb{Z}_\ell = \mathrm{Hom}_{\mathbb{Z}_\ell[\mathrm{Fr}]}(T_\ell(A), T_\ell(\tilde{A})).$$

A theorem of Tate

$$\mathrm{Hom}(A, \tilde{A}) \otimes \mathbb{Z}_\ell = \mathrm{Hom}_{\mathbb{Z}_\ell[\mathrm{Fr}]}(T_\ell(A), T_\ell(\tilde{A})).$$

In particular, A and $\tilde{A}$ are isogenous (the characteristic polynomials of Fr and $\tilde{\mathrm{Fr}}$ coincide).

Curves and their Jacobians

Let k be any field and C/k a smooth curve over k of genus $\mathrm{g}(C) \geq 2$, with $C(k) \neq \emptyset$. For each $n \in \mathbb{N}$, we have

$$(c_1, \ldots, c_n) \longrightarrow (c_1 + \cdots + c_n)$$

$$\begin{tikzcd} C^n \arrow[r] & \mathrm{Sym}^n(C) \arrow[d, "\lambda_n"] \\ & J^n \end{tikzcd}$$

Curves and their Jacobians

Let k be any field and C/k a smooth curve over k of genus $\mathrm{g}(C) \geq 2$, with $C(k) \neq \emptyset$. For each $n \in \mathbb{N}$, we have

$$(c_1, \ldots, c_n) \longrightarrow (c_1 + \cdots + c_n)$$

$$\begin{tikzcd} C^n \arrow[r] & \mathrm{Sym}^n(C) \arrow[d, "\lambda_n"] \\ & J^n \end{tikzcd}$$

Choosing $c_0 \in C(k)$, we may identify $J^n \simeq J$.

Curves and their Jacobians

Let k be any field and C/k a smooth curve over k of genus $\mathrm{g}(C) \geq 2$, with $C(k) \neq \emptyset$. For each $n \in \mathbb{N}$, we have

$$(c_1, \ldots, c_n) \longrightarrow (c_1 + \cdots + c_n)$$

$$\begin{tikzcd} C^n \arrow[r] & \mathrm{Sym}^n(C) \arrow[d, "\lambda_n"] \\ & J^n \end{tikzcd}$$

Choosing $c_0 \in C(k)$, we may identify $J^n \simeq J$.

- $\mathrm{Image}(\lambda_{\mathrm{g}-1}) = \Theta \subset J$, the Theta divisor

Curves and their Jacobians

Let k be any field and C/k a smooth curve over k of genus $\mathrm{g}(C) \geq 2$, with $C(k) \neq \emptyset$. For each $n \in \mathbb{N}$, we have

$$(c_1, \ldots, c_n) \longrightarrow (c_1 + \cdots + c_n)$$

$$\begin{tikzcd} C^n \arrow[r] & \mathrm{Sym}^n(C) \arrow[d, "\lambda_n"] \\ & J^n \end{tikzcd}$$

Choosing $c_0 \in C(k)$, we may identify $J^n \simeq J$.

- $\mathrm{Image}(\lambda_{\mathrm{g}-1}) = \Theta \subset J$, the Theta divisor
- Torelli: the pair (J, Θ) determines C, up to isomorphism

Curves and their Jacobians

Let k be any field and C/k a smooth curve over k of genus $\mathrm{g}(C) \geq 2$, with $C(k) \neq \emptyset$. For each $n \in \mathbb{N}$, we have

$$(c_1, \ldots, c_n) \longrightarrow (c_1 + \cdots + c_n)$$

$$\begin{tikzcd} C^n \arrow[r] & \mathrm{Sym}^n(C) \arrow[d, "\lambda_n"] \\ & J^n \end{tikzcd}$$

Choosing $c_0 \in C(k)$, we may identify $J^n \simeq J$.

- $\mathrm{Image}(\lambda_{\mathrm{g}-1}) = \Theta \subset J$, the Theta divisor
- Torelli: the pair (J, Θ) determines C, up to isomorphism
- for $n \geq 2\mathrm{g} - 1$, λ_n is a $\mathbb{P}^{n-\mathrm{g}}$-bundle

Let k be a finite field, $\#k \gg 1$ (e.g., $\sim 2\mathrm{g}^2$). Choose a point $x \in J(k)$.

$$\begin{tikzcd} \mathrm{Sym}^n(C)(k) \arrow[d, "\mathbb{P}_x^{n-\mathrm{g}}"] \\ J(k) \ni x \end{tikzcd}$$

Curves and their Jacobians: Equidistribution

Let k be a finite field, $\#k \gg 1$ (e.g., $\sim 2\mathrm{g}^2$). Choose a point $x \in J(k)$.

$$\begin{tikzcd} \mathrm{Sym}^n(C)(k) \arrow[d, "\mathbb{P}_x^{n-\mathrm{g}}"] \\ J(k) \ni x \end{tikzcd}$$

1. There exists a $y \in \mathbb{P}_x(k)$ such that the zero-cycle $y = c_1 + \cdots + c_n$ is completely split over k.

Curves and their Jacobians: Equidistribution

Let k be a finite field, $\#k \gg 1$ (e.g., $\sim 2g^2$). Choose a point $x \in J(k)$.

$$\begin{tikzcd} \mathrm{Sym}^n(C)(k) \arrow[d, "\mathbb{P}_x^{n-g}"] \\ J(k) \ni x \end{tikzcd}$$

1. There exists a $y \in \mathbb{P}_x(k)$ such that the zero-cycle $y = c_1 + \cdots + c_n$ is completely split over k.
2. There exists a $y \in \mathbb{P}_x(k)$ such that $y = c_1 + \cdots + c_n$ is irreducible over k.

Curves and their Jacobians: Applications

Let k be a (sufficiently large) finite field and $\bar{k}$ its algebraic closure. Recall

$$J(\bar{k}) = p\text{-part} \oplus \bigoplus_{\ell \neq p} (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}.$$

Let k be a (sufficiently large) finite field and $\bar{k}$ its algebraic closure. Recall

$$J(\bar{k}) = p\text{-part} \oplus \bigoplus_{\ell \neq p} (\mathbb{Q}_\ell / \mathbb{Z}_\ell)^{2g}.$$

1. $J(k)$ is generated by $C(k)$.

Let k be a (sufficiently large) finite field and $\bar{k}$ its algebraic closure. Recall

$$J(\bar{k}) = p\text{-part} \oplus \bigoplus_{\ell \neq p} (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}.$$

1. $J(k)$ is generated by $C(k)$.
2. $J(\bar{k}) = \bigcup_{n \in \mathbb{N}} n \cdot C(\bar{k})$.

Curves and their Jacobians

Let

$$k = k_1 \subset k_2 \subset \ldots \subset k_n \subset \ldots$$

be the tower of degree 2 extensions.

Curves and their Jacobians

Let

$$k = k_1 \subset k_2 \subset \ldots \subset k_n \subset \ldots$$

be the tower of degree 2 extensions.

Let C be a nonhyperelliptic curve of genus $\mathrm{g}(C) \geq 3$. By (1), to characterize $J(k_n)$ it suffices to characterize $C(k_n)$.

Let

$$k = k_1 \subset k_2 \subset \ldots \subset k_n \subset \ldots$$

be the tower of degree 2 extensions.
Let C be a nonhyperelliptic curve of genus $g(C) \geq 3$. By (1), to characterize $J(k_n)$ it suffices to characterize $C(k_n)$.

Inductive characterization of $J(k_n)$, $n \in \mathbb{N}$

$J(k_n)$ is generated by points $c \in C(\bar{k})$ such that

- $c \notin C(k_{n-1})$
- there exists a point $c' \in C(\bar{k})$ with

$$c + c' \in J(k_{n-1}).$$

Curves and their Jacobians

Let $\tilde{C}$ be another smooth projective curve and $\tilde{J}$ its Jacobian. Isomorphism of pairs:

$$\phi : (C, J) \to (\tilde{C}, \tilde{J})$$

$$\begin{tikzcd} J(\bar{k}) \arrow[d, "\phi^0"'] & J^1(\bar{k}) \arrow[d, "\phi^1"'] & C(\bar{k}) \arrow[l, "j_1"'] \arrow[d, "\phi_s"'] \\ \tilde{J}(\bar{k}) & \tilde{J}^1(\bar{k}) & \tilde{C}(\bar{k}) \arrow[l, "\tilde{j}_1"'] \end{tikzcd}$$

where

- ϕ^0: isomorphism of abstract abelian groups;
- ϕ^1: isomorphism of homogeneous spaces, compatible with ϕ^0;
- the restriction $\phi_s : C(\bar{k}) \to \tilde{C}(\bar{k})$ of ϕ^1 is a bijection of sets.

Curves and their Jacobians: Torelli

Theorem

Let $(C, J) \to (\tilde{C}, \tilde{J})$ be an isomorphism of pairs. Then J is isogenous to $\tilde{J}$.

Theorem

Let $(C, J) \to (\tilde{C}, \tilde{J})$ be an isomorphism of pairs. Then J is isogenous to $\tilde{J}$.

Proof.

1. Choose $k_1, \tilde{k_1}$ (sufficiently large) such that $\phi(J(k_1)) \subset \tilde{J}(\tilde{k}_1)$

Curves and their Jacobians: Torelli

Theorem

Let $(C, J) \to (\tilde{C}, \tilde{J})$ be an isomorphism of pairs. Then J is isogenous to $\tilde{J}$.

Proof.

1. Choose $k_1, \tilde{k}_1$ (sufficiently large) such that $\phi(J(k_1)) \subset \tilde{J}(\tilde{k}_1)$
2. Define $C(k_n)$, resp. $\tilde{C}(\tilde{k}_n)$, intrinsically, as above.

Curves and their Jacobians: Torelli

Theorem

Let $(C, J) \to (\tilde{C}, \tilde{J})$ be an isomorphism of pairs. Then J is isogenous to $\tilde{J}$.

Proof.

1. Choose $k_1, \tilde{k_1}$ (sufficiently large) such that $\phi(J(k_1)) \subset \tilde{J}(\tilde{k}_1)$
2. Define $C(k_n)$, resp. $\tilde{C}(\tilde{k}_n)$, intrinsically, as above.
3. Have $\phi(J(k_n)) \subset \tilde{J}(\tilde{k}_n)$, for all $n \in \mathbb{N}$.

Theorem

Let $(C, J) \to (\tilde{C}, \tilde{J})$ be an isomorphism of pairs. Then J is isogenous to $\tilde{J}$.

Proof.

1. Choose $k_1, \tilde{k_1}$ (sufficiently large) such that $\phi(J(k_1)) \subset \tilde{J}(\tilde{k}_1)$
2. Define $C(k_n)$, resp. $\tilde{C}(\tilde{k}_n)$, intrinsically, as above.
3. Have $\phi(J(k_n)) \subset \tilde{J}(\tilde{k}_n)$, for all $n \in \mathbb{N}$.
4. $\#J(k_n) \mid \#\tilde{J}(\tilde{k}_n)$

Theorem

Let $(C, J) \to (\tilde{C}, \tilde{J})$ be an isomorphism of pairs. Then J is isogenous to $\tilde{J}$.

Proof.

1. Choose $k_1, \tilde{k_1}$ (sufficiently large) such that $\phi(J(k_1)) \subset \tilde{J}(\tilde{k}_1)$
2. Define $C(k_n)$, resp. $\tilde{C}(\tilde{k}_n)$, intrinsically, as above.
3. Have $\phi(J(k_n)) \subset \tilde{J}(\tilde{k}_n)$, for all $n \in \mathbb{N}$.
4. $\#J(k_n) \mid \#\tilde{J}(\tilde{k}_n)$
5. Apply the result about recurrence sequences.

Specifying the curve

n-string: an ordered set $S_n = \{s_1, \ldots, s_n\}$ of integers $s_j > 1$, with $p \nmid s_j$ for all j.

Specifying the curve

n-string: an ordered set $S_n = \{s_1, \ldots, s_n\}$ of integers $s_j > 1$, with $p \nmid s_j$ for all j.
S_n-configuration on $C(k)$': ordered subset $\{c_0, c_1, \ldots, c_n\} \subset C(k)$ such that $\mathrm{ord}(c_j - c_0) = s_j$, for all j.

Specifying the curve

n-string: an ordered set $S_n = \{s_1, \ldots, s_n\}$ of integers $s_j > 1$, with $p \nmid s_j$ for all j.

S_n-configuration on $C(k)$': ordered subset $\{c_0, c_1, \ldots, c_n\} \subset C(k)$ such that $\mathrm{ord}(c_j - c_0) = s_j$, for all j.

Specifying the curve

n-string: an ordered set $S_n = \{s_1, \dots, s_n\}$ of integers $s_j > 1$, with $p \nmid s_j$ for all j.
S_n-configuration on $C(k)$': ordered subset $\{c_0, c_1, \dots, c_n\} \subset C(k)$ such that $\mathrm{ord}(c_j - c_0) = s_j$, for all j.

Theorem

Let C be a curve over $k = \bar{\mathbb{F}}_p$ of genus $\mathrm{g} > 1$. Then there exists a string S_n, with $n < 2\mathrm{g}$ such that

- *$C(k) \subset J(k)$ contains an S_n-configuration,*
- *there exist at most finitely many nonisomorphic curves of genus g containing an S_n-configuration, modulo Frobenius twists.*

Reconstructing the isogeny

Let

$$\phi : (C, J) \to (\tilde{C}, \tilde{J})$$

be an isomorphism of pairs.

Theorem

Some powers of the endomorphisms $\phi(\mathrm{Fr}), \tilde{\mathrm{Fr}} \in \mathrm{End}(\tilde{J})$ *commute.*

Applications to anabelian geometry

Let $k = \bar{\mathbb{F}}_p$ and $K = k(C)$. Let G_K be the absolute Galois group of K. Let

$$\mathcal{I}_K := \{\mathcal{I}_\nu^a\},$$

the set of inertia subgroups $\mathcal{I}_\nu^a \subset G_K^a$ of nontrivial divisorial valuations of K (i.e., points of C).

Theorem

Assume that $\mathrm{g}(C) > 2$ *and that*

$$(G_K^a, \mathcal{I}_K) \simeq (G_{\tilde{K}}^a, \mathcal{I}_{\tilde{K}}).$$

Then

$$J \sim \tilde{J}.$$

Curves and their Jacobians

$$\begin{array}{c} \mathrm{Sym}^n(C)(k) \\ \Big\downarrow \mathbb{P}_x^{n-g} \\ J(k) \ni x \end{array}$$

Recall that there exist

$$y = c_1 + \cdots + c_n \in \mathbb{P}_x^{n-g}(k)$$

such that the zero-cycle is k-irreducible.

Curves and their Jacobians

$$\begin{array}{c} \mathrm{Sym}^n(C)(k) \\ \Big\downarrow \scriptstyle{\mathbb{P}_x^{n-g}} \\ J(k) \ni x \end{array}$$

Recall that there exist

$$y = c_1 + \cdots + c_n \in \mathbb{P}_x^{n-g}(k)$$

such that the zero-cycle is k-irreducible. Then

$$x = \sum_{i=1}^{n} \mathrm{Fr}^j(c_1) \in J(\bar{k}).$$

Curves and their Jacobians

Lift Fr to an element in $\mathrm{End}_k(J)$ and put

$$\Psi := \sum_{i=1}^{n} \mathrm{Fr}^j.$$

Then $x = \Psi(c_1)$ and

$$J(k) \subset \Psi(C)(\bar{k}).$$

Curves and their Jacobians

Lift Fr to an element in $\mathrm{End}_k(J)$ and put

$$\Psi := \sum_{i=1}^{n} \mathrm{Fr}^j.$$

Then $x = \Psi(c_1)$ and

$$J(k) \subset \Psi(C)(\bar{k}).$$

For any finite set of points $x_1, \ldots, x_r \in J(\bar{k})$ we can find a Ψ such that

$$\{x_1, \ldots, x_r\} \subset \Psi(C)(\bar{k}).$$

Curves and their Jacobians

Lift Fr to an element in $\mathrm{End}_k(J)$ and put

$$\Psi := \sum_{i=1}^{n} \mathrm{Fr}^j.$$

Then $x = \Psi(c_1)$ and

$$J(k) \subset \Psi(C)(\bar{k}).$$

For any finite set of points $x_1, \ldots, x_r \in J(\bar{k})$ we can find a Ψ such that

$$\{x_1, \ldots, x_r\} \subset \Psi(C)(\bar{k}).$$

A similar argument allows to replace Ψ by the endomorphism multiplication by n.

K3 surfaces in positive characteristic

Let $X = \widetilde{A/G}$ be a Kummer K3 surface: a desingularization of the quotient of an abelian surface by the action of a finite group $G = \mathbb{Z}/2, \mathbb{Z}/3, \ldots$ (there is a finite list of groups and actions).

For example,

$$X \,:\, \sum_{i=0}^{3} x_i^4 = 0.$$

K3 surfaces in positive characteristic

Let $X = \widetilde{A/G}$ be a Kummer K3 surface: a desingularization of the quotient of an abelian surface by the action of a finite group $G = \mathbb{Z}/2, \mathbb{Z}/3, \ldots$ (there is a finite list of groups and actions).

For example,

$$X : \sum_{i=0}^{3} x_i^4 = 0.$$

A Kummer K3 surface X is uniruled (or unirational) iff X is supersingular, i.e., A is supersingular (Shioda, Katsura).

Theorem (Rudakov-Shafarevich)

If the characteristic of k equals 2 then a K3 surface is supersingular if and only if it is unirational.

Theorem (Bogomolov-T. 2005)

Let $X = \widetilde{A/G}$ be a Kummer surface defined over a (sufficiently large) finite field k. For every finite set of algebraic points $\{x_1, \dots, x_n\}$ in the complement to exceptional curves there exists a geometrically irreducible rational curve R, defined over k, with

$$\{x_1, \dots, x_n\} \subset R(\bar{k}).$$

Theorem (Bogomolov-T. 2005)

Let $X = \widetilde{A/G}$ be a Kummer surface defined over a (sufficiently large) finite field k. For every finite set of algebraic points $\{x_1, \ldots, x_n\}$ in the complement to exceptional curves there exists a geometrically irreducible rational curve R, defined over k, with

$$\{x_1, \ldots, x_n\} \subset R(\bar{k}).$$

This gives examples of "rationally connected", non-uniruled K3 surfaces over finite fields.

Proof

Let $G = \mathbb{Z}/2$, and let k be sufficiently large, finite. Let C be a hyperelliptic curve of genus 2, fix $c_0 \in C(k)$ (a ramification point under the standard involution). We have an embedding

$$\begin{array}{ccc} C & \hookrightarrow & A \\ c & \mapsto & c - c_0 \end{array}$$

into the Jacobian A of C. We know that $A(\bar{k}) = \cup_n n \cdot C(\bar{k})$. The image of C in A/G is a rational curve.

Proof

Let $G = \mathbb{Z}/2$, and let k be sufficiently large, finite. Let C be a hyperelliptic curve of genus 2, fix $c_0 \in C(k)$ (a ramification point under the standard involution). We have an embedding

$$\begin{array}{ccc} C & \hookrightarrow & A \\ c & \mapsto & c - c_0 \end{array}$$

into the Jacobian A of C. We know that $A(\bar{k}) = \cup_n n \cdot C(\bar{k})$. The image of C in A/G is a rational curve. Same holds for the images of $n \cdot C$.

Proof

Let $G = \mathbb{Z}/2$, and let k be sufficiently large, finite. Let C be a hyperelliptic curve of genus 2, fix $c_0 \in C(k)$ (a ramification point under the standard involution). We have an embedding

$$\begin{array}{ccc} C & \hookrightarrow & A \\ c & \mapsto & c - c_0 \end{array}$$

into the Jacobian A of C. We know that $A(\bar{k}) = \cup_n n \cdot C(\bar{k})$. The image of C in A/G is a rational curve. Same holds for the images of $n \cdot C$. Thus every algebraic point on X lies on a rational curve.

Proof

Let $G = \mathbb{Z}/2$, and let k be sufficiently large, finite. Let C be a hyperelliptic curve of genus 2, fix $c_0 \in C(k)$ (a ramification point under the standard involution). We have an embedding

$$\begin{array}{ccc} C & \hookrightarrow & A \\ c & \mapsto & c - c_0 \end{array}$$

into the Jacobian A of C. We know that $A(\bar{k}) = \cup_n n \cdot C(\bar{k})$. The image of C in A/G is a rational curve. Same holds for the images of $n \cdot C$. Thus every algebraic point on X lies on a rational curve. Similar arguments work for finitely many points and other groups G.

Proof

Let $G = \mathbb{Z}/2$, and let k be sufficiently large, finite. Let C be a hyperelliptic curve of genus 2, fix $c_0 \in C(k)$ (a ramification point under the standard involution). We have an embedding

$$\begin{array}{ccc} C & \hookrightarrow & A \\ c & \mapsto & c - c_0 \end{array}$$

into the Jacobian A of C. We know that $A(\bar{k}) = \cup_n n \cdot C(\bar{k})$. The image of C in A/G is a rational curve. Same holds for the images of $n \cdot C$. Thus every algebraic point on X lies on a rational curve. Similar arguments work for finitely many points and other groups G.

Same for Calabi-Yau varieties built from abelian varieties or K3 surfaces.

Surfaces of general type

We work over a finite field of characteristic ≥ 3. Consider the diagram

$$\begin{array}{ccc} X_1 & \rightarrow & X \\ \downarrow & & \downarrow \\ \mathbb{P}^2 & \rightarrow & X_0 \end{array},$$

where

- X_0 is a unirational surface of general type, $\mathbb{P}^2 \rightarrow X_0$
- $X_1 \rightarrow \mathbb{P}^2$ is a double cover ramified in a curve of degree 6; it is a K3 surface. Moreover, we may assume that X_1 is a non-supersingular (and thus non-uniruled) Kummer surface.

Surfaces of general type

We work over a finite field of characteristic ≥ 3. Consider the diagram

$$\begin{array}{ccc} X_1 & \to & X \\ \downarrow & & \downarrow \\ \mathbb{P}^2 & \to & X_0 \end{array},$$

where

- X_0 is a unirational surface of general type, $\mathbb{P}^2 \to X_0$
- $X_1 \to \mathbb{P}^2$ is a double cover ramified in a curve of degree 6; it is a K3 surface. Moreover, we may assume that X_1 is a non-supersingular (and thus non-uniruled) Kummer surface.

Then X is

- rationally connected,
- of general type,
- non-uniruled.