Algebraic varieties over small fields

Mathematisches Institut

July 30, 2006

Small fields

- Small fields: $k = \mathbb{F}_q, \mathbb{Q}, \mathbb{C}(t), \ldots$
- X smooth projective algebraic variety over k

Small fields

- Small fields: $k = \mathbb{F}_q, \mathbb{Q}, \mathbb{C}(t), \ldots$
- X smooth projective algebraic variety over k

We are interested in:

- rational points $X(k)$
- algebraic points $X(\bar{k})$
- rational curves on X and their relation to arithmetic properties of X

Classification via degree

1. low degree: Fano
2. high degree: general type
3. intermediate type

Classification via degree

1. low degree: Fano
2. high degree: general type
3. intermediate type

Basic examples:

1. $X_d \subset \mathbb{P}^n$, with $d \leq n$: quadrics, cubic surfaces
2. X_d with $d \geq n+2$
3. X_d with $d = n+1$: K3 surfaces (quartic in $\mathbb{P}^3$, intersection of three quadrics in $\mathbb{P}^5$), abelian varieties, Calabi-Yau varieties

Classification via degree

1. low degree: Fano
2. high degree: general type
3. intermediate type

Basic examples:

1. $X_d \subset \mathbb{P}^n$, with $d \leq n$: quadrics, cubic surfaces
2. X_d with $d \geq n+2$
3. X_d with $d = n+1$: K3 surfaces (quartic in $\mathbb{P}^3$, intersection of three quadrics in $\mathbb{P}^5$), abelian varieties, Calabi-Yau varieties

More intrinsically, classification by the ampleness of the canonical class.

Birational classification

How close is X to the basic projective variety: $\mathbb{P}^n$:

- rational $=$ birational to $\mathbb{P}^n$
- unirational $=$ dominated by $\mathbb{P}^n$
- uniruled $=$ dominated by $Y \times \mathbb{P}^1$, with $\dim(Y) = \dim(X) - 1$
- stably rational etc.

Birational classification

How close is X to the basic projective variety: $\mathbb{P}^n$:

- rational = birational to $\mathbb{P}^n$
- unirational = dominated by $\mathbb{P}^n$
- uniruled = dominated by $Y \times \mathbb{P}^1$, with $\dim(Y) = \dim(X) - 1$
- stably rational etc.

These properties depend on the field.

Birational classification

How close is X to the basic projective variety: $\mathbb{P}^n$:

- rational $=$ birational to $\mathbb{P}^n$
- unirational $=$ dominated by $\mathbb{P}^n$
- uniruled $=$ dominated by $Y \times \mathbb{P}^1$, with $\dim(Y) = \dim(X) - 1$
- stably rational etc.

These properties depend on the field.
Small degree surfaces (Fano surfaces) over algebraically closed fields are rational. Cubic surfaces with a rational point are unirational.

Rational connectivity

Let X be a variety over an algebraically closed field k. When $X = \mathbb{P}^n$, every pair of points can be connected by a line. Any finite set of points can be connected by a rational curve.

Rational connectivity

Let X be a variety over an algebraically closed field k. When $X = \mathbb{P}^n$, every pair of points can be connected by a line. Any finite set of points can be connected by a rational curve.

In general, we have (at least) two notions of connectivity via rational curves:

(1) For all $x_1, x_2 \in X(k)$ there exists a chain of rational curves $C_1 \cup \ldots \cup C_r \subset X$ connecting x_1 and x_2;

(2) For all $x_1, x_2 \in X(k)$ there exists a *free* rational curve $C \subset X$ connecting x_1, x_2.

(3) Same for a finite set of points.

Rational connectivity

Let X be a variety over an algebraically closed field k. When $X = \mathbb{P}^n$, every pair of points can be connected by a line. Any finite set of points can be connected by a rational curve.

In general, we have (at least) two notions of connectivity via rational curves:

(1) For all $x_1, x_2 \in X(k)$ there exists a chain of rational curves $C_1 \cup \ldots \cup C_r \subset X$ connecting x_1 and x_2;

(2) For all $x_1, x_2 \in X(k)$ there exists a *free* rational curve $C \subset X$ connecting x_1, x_2.

(3) Same for a finite set of points.

For smooth projective X these are equivalent and birational properties. The situation is less clear for quasi-projective X:

Question

Does (2) hold for the smooth locus of a partial desingularization of singular cubic surface?

Rational curves

Theorem

Smooth Fano varieties are rationally connected.

Rational curves

Theorem

Smooth Fano varieties are rationally connected.

Theorem (Esnault 2001)

Every smooth rationally connected variety over a finite field has a rational point.

Theorem (Graber-Harris-Starr 2001)

Every smooth rationally connected variety X over $k = \mathbb{C}(t)$ has a rational point. Moreover, $X(k)$ is Zariski dense.

Rational curves II

- A surface of general type over $\mathbb{C}$ should have at most finitely many rational curves.
- Abelian varieties don't contain rational curves.
- Counting rational curves on Calabi-Yau varieties is an interesting problem.

Rational curves II

- A surface of general type over $\mathbb{C}$ should have at most finitely many rational curves.
- Abelian varieties don't contain rational curves.
- Counting rational curves on Calabi-Yau varieties is an interesting problem.
- A general K3 surface over $\mathbb{C}$ contains infinitely many rational curves. It is not known whether every K3 surface over $\bar{\mathbb{Q}}$ or $\bar{\mathbb{F}}_p$ contains infinitely many rational curves.

Rational curves II

- A surface of general type over $\mathbb{C}$ should have at most finitely many rational curves.
- Abelian varieties don't contain rational curves.
- Counting rational curves on Calabi-Yau varieties is an interesting problem.
- A general K3 surface over $\mathbb{C}$ contains infinitely many rational curves. It is not known whether every K3 surface over $\bar{\mathbb{Q}}$ or $\bar{\mathbb{F}}_p$ contains infinitely many rational curves.
- Varieties of rational curves of fixed degree on Fano varieties carry interesting geometric information (variety of lines on a cubic fourfolds is diffeomorphic to a symmetric square of a K3 surface).

Rational curves II

- A surface of general type over $\mathbb{C}$ should have at most finitely many rational curves.
- Abelian varieties don't contain rational curves.
- Counting rational curves on Calabi-Yau varieties is an interesting problem.
- A general K3 surface over $\mathbb{C}$ contains infinitely many rational curves. It is not known whether every K3 surface over $\bar{\mathbb{Q}}$ or $\bar{\mathbb{F}}_p$ contains infinitely many rational curves.
- Varieties of rational curves of fixed degree on Fano varieties carry interesting geometric information (variety of lines on a cubic fourfolds is diffeomorphic to a symmetric square of a K3 surface).

In positive characteristic, there exist unirational surfaces of general type:

$$x^{p+1} + y^{p+1} + z^{p+1} + t^{p+1} = 0$$

is unirational in characteristic p and is of general type for $p \geq 5$.

Abelian varieties

Every abelian surface is isogenous to the Jacobian of a hyperelliptic curve of genus 2.

Abelian varieties

Every abelian surface is isogenous to the Jacobian of a hyperelliptic curve of genus 2.

Theorem

- Pirola (1989): a generic abelian variety of dimension ≥ 3 over $\mathbb{C}$ does not contain hyperelliptic curves.

Abelian varieties

Every abelian surface is isogenous to the Jacobian of a hyperelliptic curve of genus 2.

Theorem

- Pirola (1989): a generic abelian variety of dimension ≥ 3 over $\mathbb{C}$ does not contain hyperelliptic curves.
- de Jong, Oort (1996): same over large fields of positive characteristic

Question

Let k be the closure of a finite field. Is A dominated by the Jacobian of a hyperelliptic curve?

Curves and their Jacobians

Let C be a smooth projective curve of genus $\mathrm{g}(C) \geq 2$ over a finite field k. Assume that $C(k) \neq \emptyset$. Fix a point $c_0 \in C(k)$ and the embedding

$$\begin{array}{ccc} C & \hookrightarrow & J = J_C \\ c & \mapsto & c - c_0 \end{array}.$$

Curves and their Jacobians

Let C be a smooth projective curve of genus $\mathrm{g}(C) \geq 2$ over a finite field k. Assume that $C(k) \neq \emptyset$. Fix a point $c_0 \in C(k)$ and the embedding

$$\begin{array}{ccc} C & \hookrightarrow & J = J_C \\ c & \mapsto & c - c_0 \end{array}.$$

Put

- $J\{\ell\} := \cup_{n \in \mathbb{N}} J(\bar{k})[\ell^n]$ - the ℓ-primary part of $J(\bar{k})$
- S - a finite set of primes
- $\lambda_S : J(\bar{k}) \to J\{S\} := \prod_{\ell \in S} J\{\ell\}$ - the projection

Curves and their Jacobians II

Theorem (Bogomolov-T. 2005)

Let C be a smooth projective curve over a finite field k of genus ≥ 2. Let A be an abelian variety containing C. Assume that C generates A (i.e., $J = J_C$ surjects onto A). Then

$$A(\bar{k}) = \cup_{m=1 \bmod n} \, m \cdot C(\bar{k}), \quad \text{for all} \quad n \in \mathbb{N}.$$

Curves and their Jacobians II

Theorem (Bogomolov-T. 2005)

Let C be a smooth projective curve over a finite field k of genus ≥ 2. Let A be an abelian variety containing C. Assume that C generates A (i.e., $J = J_C$ surjects onto A). Then

$$A(\bar{k}) = \cup_{m=1 \bmod n} \; m \cdot C(\bar{k}), \quad \text{for all} \quad n \in \mathbb{N}.$$

- Similar result for semi-abelian varieties.

Curves and their Jacobians II

Theorem (Bogomolov-T. 2005)

Let C be a smooth projective curve over a finite field k of genus ≥ 2. Let A be an abelian variety containing C. Assume that C generates A (i.e., $J = J_C$ surjects onto A). Then

$$A(\bar{k}) = \cup_{m=1 \bmod n}\, m \cdot C(\bar{k}), \quad \text{for all} \quad n \in \mathbb{N}.$$

- Similar result for semi-abelian varieties.
- Given $a \in A(\bar{k})$, how to compute m?

Curves and their Jacobians II

Theorem (Bogomolov-T. 2005)

Let C be a smooth projective curve over a finite field k of genus ≥ 2. Let A be an abelian variety containing C. Assume that C generates A (i.e., $J = J_C$ surjects onto A). Then

$$A(\bar{k}) = \cup_{m=1 \bmod n} \, m \cdot C(\bar{k}), \quad \text{for all} \quad n \in \mathbb{N}.$$

- Similar result for semi-abelian varieties.
- Given $a \in A(\bar{k})$, how to compute m?
- Applications to cryptography?

Curves and their Jacobians III

Theorem (Bogomolov-T. 2005)

Let S be a finite set of primes. There exists an infinite set of primes Π containing S, of positive density, such that

$$\lambda_S : C(\bar{k}) \to \oplus_{\ell \in \Pi} A\{\ell\}$$

is surjective.

Sketch of proof

Consider the maps

$$\begin{array}{ccccc} C^n & \xrightarrow{\phi_n} & \mathrm{Sym}^{(n)}(C) & & \\ & & \downarrow & & \mathbb{P}_x^{n-g} \\ & & J^{(k)} = J(k) & \ni x, & \end{array}$$

for $n \geq 2g + 1$.

Sketch of proof

Consider the maps

$$
\begin{array}{ccccc}
C^n & \xrightarrow{\phi_n} & \mathrm{Sym}^{(n)}(C) & & \\
 & & \downarrow & & \mathbb{P}_x^{n-g} \\
 & & J^{(k)} = J(k) & \ni & x,
\end{array}
$$

for $n \geq 2g + 1$.

Lemma

For k large enough, there exists a $y \in \mathbb{P}_x^{n-g}(k)$ such that the cycle $c_1 + \cdots + c_n = \phi_n^{-1}(y)$ is irreducible over k.

Sketch of proof

Consider the maps

$$\begin{array}{ccccc} C^n & \xrightarrow{\phi_n} & \mathrm{Sym}^{(n)}(C) & & \\ & & \downarrow & & \mathbb{P}_x^{n-g} \\ & & J^{(k)} = J(k) & \ni x, & \end{array}$$

for $n \geq 2g + 1$.

Lemma

For k large enough, there exists a $y \in \mathbb{P}_x^{n-g}(k)$ such that the cycle $c_1 + \cdots + c_n = \phi_n^{-1}(y)$ is irreducible over k.

It follows that

$$y = \sum_{j=1}^{n} \mathrm{Fr}^j(c_1).$$

Sketch of proof II

Lifting Fr to an element $\tilde{\mathrm{Fr}} \in \mathrm{End}_k(A)$, we obtain

$$y = \Psi(c_1), \quad \text{where} \quad \Psi := \sum_{j=1}^{n} \tilde{\mathrm{Fr}}^j \in \mathrm{End}_k(A).$$

Sketch of proof II

Lifting Fr to an element $\tilde{\mathrm{Fr}} \in \mathrm{End}_k(A)$, we obtain

$$y = \Psi(c_1), \quad \text{where} \quad \Psi := \sum_{j=1}^{n} \tilde{\mathrm{Fr}}^j \in \mathrm{End}_k(A).$$

Moreover, for any finite set of points $x_1, \ldots, x_r \in A(k)$ we find

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

Sketch of proof II

Lifting Fr to an element $\tilde{\mathrm{Fr}} \in \mathrm{End}_k(A)$, we obtain

$$y = \Psi(c_1), \quad \text{where} \quad \Psi := \sum_{j=1}^{n} \tilde{\mathrm{Fr}}^j \in \mathrm{End}_k(A).$$

Moreover, for any finite set of points $x_1, \ldots, x_r \in A(k)$ we find

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

A similar argument allows to replace $\Psi \in \mathrm{End}_k(A)$ by the endomorphism multiplication by n $\in \mathrm{End}_k(A)$.

Points in towers

Let k be a finite field, S a finite set of primes and k_S the field extension generated by $J\{S\}$-points.

Boxall (1992)

$$C(k_S) \cap J\{S\} \quad \text{is finite}$$

Recall: $\lambda_S : C(k_S) \to J\{S\}$ is surjective.

Points in towers

Let k be a finite field, S a finite set of primes and k_S the field extension generated by $J\{S\}$-points.

Boxall (1992)

$$C(k_S) \cap J\{S\} \quad \text{is finite}$$

Recall: $\lambda_S : C(k_S) \to J\{S\}$ is surjective.
Intuition: To get points in $C(k_S)$ of orders divisible by high powers of ℓ, for $\ell \in S$, we need to increase the number of factors outside S.

ABC over finite fields

For $c \in C(\bar{k}) \hookrightarrow J(\bar{k})$, let

- $\Delta(c)$ be the order of c in $J(\bar{k})$ and
- $\mathfrak{f}(c) = \prod_{\ell | \Delta(c)} \ell$ be the conductor

These invariants depend on the embedding $C \hookrightarrow J$.

Conjecture

For all $\epsilon > 0$ one has
$$\Delta(c) = O(\mathfrak{f}(c)^{1+\epsilon}).$$

K3 surfaces

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

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.

Kummer surfaces over finite fields

Theorem (Bogomolov-T. 2005)

Assume that X is defined over a finite field k. Then there exists a finite extension k'/k such that for every finite set of algebraic points $\{x_1, \dots, x_n\} \subset X^\circ(\bar{k})$ in the complement to exceptional curves there exists an geometrically irreducible rational curve C, defined over k', with

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

Kummer surfaces over finite fields

Theorem (Bogomolov-T. 2005)

Assume that X is defined over a finite field k. Then there exists a finite extension k'/k such that for every finite set of algebraic points $\{x_1, \ldots, x_n\} \subset X^\circ(\bar{k})$ in the complement to exceptional curves there exists an geometrically irreducible rational curve C, defined over k', with

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

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.
A similar argument works for finitely many points and other groups G.

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.

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.

Number fields

Let $X = A/G$ be a Kummer K3 surface, with A the Jacobian of a genus 2 curve C and $G = \mathbb{Z}/2$, over a number field k. Assume c_0 (from before) is defined over k. Fix a good model over $\mathrm{Spec}(\mathcal{O}_k)$. Let S be a finite set of places of good reduction. For $v \in S$, choose a point $\tilde{x}_v \in X(\mathbb{F}_v)$.

Theorem (Bogomolov-T. 2005)

There exists a rational point $x \in X(k)$ such that for all $v \in S$,

$$x_v = \tilde{x}_v.$$

Number fields

Let $X = A/G$ be a Kummer K3 surface, with A the Jacobian of a genus 2 curve C and $G = \mathbb{Z}/2$, over a number field k. Assume c_0 (from before) is defined over k. Fix a good model over $\mathrm{Spec}(\mathcal{O}_k)$. Let S be a finite set of places of good reduction. For $v \in S$, choose a point $\tilde{x}_v \in X(\mathbb{F}_v)$.

Theorem (Bogomolov-T. 2005)

There exists a rational point $x \in X(k)$ such that for all $v \in S$,

$$x_v = \tilde{x}_v.$$

This a version of weak approximation - approximation of first order jets.

Number fields

Let $X = A/G$ be a Kummer K3 surface, with A the Jacobian of a genus 2 curve C and $G = \mathbb{Z}/2$, over a number field k. Assume c_0 (from before) is defined over k. Fix a good model over $\mathrm{Spec}(\mathcal{O}_k)$. Let S be a finite set of places of good reduction. For $v \in S$, choose a point $\tilde{x}_v \in X(\mathbb{F}_v)$.

Theorem (Bogomolov-T. 2005)

There exists a rational point $x \in X(k)$ such that for all $v \in S$,

$$x_v = \tilde{x}_v.$$

This a version of weak approximation - approximation of first order jets. This property is not known for cubic surfaces (or threefolds) over number fields.

Some questions

Let $X \subset \mathbb{P}^3$ be a cubic surface over $\mathbb{Z}$, with mild singularities (rational double points). Assume that $X(\mathbb{Q}) = X(\mathbb{Z}) \neq \emptyset$.

1. Given finitely many points $x_1, \ldots, x_n \in X(\mathbb{Q})$ find a geometrically irreducible rational curve, defined over $\mathbb{Q}$, which avoids the singularities of X, and passes through $x_1, \ldots, x_n$ (interpolation).

Some questions

Let $X \subset \mathbb{P}^3$ be a cubic surface over $\mathbb{Z}$, with mild singularities (rational double points). Assume that $X(\mathbb{Q}) = X(\mathbb{Z}) \neq \emptyset$.

1. Given finitely many points $x_1, \ldots, x_n \in X(\mathbb{Q})$ find a geometrically irreducible rational curve, defined over $\mathbb{Q}$, which avoids the singularities of X, and passes through $x_1, \ldots, x_n$ (interpolation).
2. Fix a finite set S of primes of good reduction and for each $p \in S$ a point $\tilde{x}_p \in X(\mathbb{Z}/p)$. Find $x \in X(\mathbb{Z})$ with $x_p = \tilde{x}_p$ for all $p \in S$.

Some questions

Let $X \subset \mathbb{P}^3$ be a cubic surface over $\mathbb{Z}$, with mild singularities (rational double points). Assume that $X(\mathbb{Q}) = X(\mathbb{Z}) \neq \emptyset$.

1. Given finitely many points $x_1, \ldots, x_n \in X(\mathbb{Q})$ find a geometrically irreducible rational curve, defined over $\mathbb{Q}$, which avoids the singularities of X, and passes through $x_1, \ldots, x_n$ (interpolation).
2. Fix a finite set S of primes of good reduction and for each $p \in S$ a point $\tilde{x}_p \in X(\mathbb{Z}/p)$. Find $x \in X(\mathbb{Z})$ with $x_p = \tilde{x}_p$ for all $p \in S$.
3. Compile data on points of smallest height in families of cubic surfaces.

Some questions

Let $X \subset \mathbb{P}^3$ be a cubic surface over $\mathbb{Z}$, with mild singularities (rational double points). Assume that $X(\mathbb{Q}) = X(\mathbb{Z}) \neq \emptyset$.

1. Given finitely many points $x_1, \ldots, x_n \in X(\mathbb{Q})$ find a geometrically irreducible rational curve, defined over $\mathbb{Q}$, which avoids the singularities of X, and passes through $x_1, \ldots, x_n$ (interpolation).
2. Fix a finite set S of primes of good reduction and for each $p \in S$ a point $\tilde{x}_p \in X(\mathbb{Z}/p)$. Find $x \in X(\mathbb{Z})$ with $x_p = \tilde{x}_p$ for all $p \in S$.
3. Compile data on points of smallest height in families of cubic surfaces.
4. Implement an algorithm computing $\mathrm{rk}\,\mathrm{Pic}(X)$ and the action of the Galois group of a splitting field of X on the 27 lines.

Some questions

Let $X \subset \mathbb{P}^3$ be a cubic surface over $\mathbb{Z}$, with mild singularities (rational double points). Assume that $X(\mathbb{Q}) = X(\mathbb{Z}) \neq \emptyset$.

1. Given finitely many points $x_1, \ldots, x_n \in X(\mathbb{Q})$ find a geometrically irreducible rational curve, defined over $\mathbb{Q}$, which avoids the singularities of X, and passes through $x_1, \ldots, x_n$ (interpolation).
2. Fix a finite set S of primes of good reduction and for each $p \in S$ a point $\tilde{x}_p \in X(\mathbb{Z}/p)$. Find $x \in X(\mathbb{Z})$ with $x_p = \tilde{x}_p$ for all $p \in S$.
3. Compile data on points of smallest height in families of cubic surfaces.
4. Implement an algorithm computing $\mathrm{rk}\,\mathrm{Pic}(X)$ and the action of the Galois group of a splitting field of X on the 27 lines.

Let $X \subset \mathbb{P}^3$ be a quartic K3 surface over $\mathbb{Q}$. How to compute $\mathrm{rk}\,\mathrm{Pic}(X_{\bar{\mathbb{Q}}})$ effectively? The geometric rank?