K3 surfaces with Picard number one and infinitely many rational points.

Queen's University

Kingston

October 7, 2005

Ronald van Luijk

CRM, Montreal
MSRI, Berkeley

1. Motivation

2. Definitions

3. Open problems leading to our problem

4. What was known

5. Solution of our problem

Motivation from Diophantine equations

Example:
Noam Elkies found the following identity.

$$95800^4 + 217519^4 + 414560^4 = 422481^4$$

The equation $x^4 + y^4 + z^4 = t^4$ describes a surface in projective threespace $\mathbb{P}^3$. Elkies proved that the rational points are dense.

Some definitions

In this talk, a *surface* will always be smooth, projective, and geometrically integral.

A *K3 surface* is a surface X with $\dim H^1(X, \mathcal{O}_X) = 0$ on which the canonical sheaf is trivial.

Examples:

- A smooth quartic surface in $\mathbb{P}^3$.
- If A is an abelian surface, then the minimal nonsingular model of $A/[-1]$ is a K3 surface. Such surfaces are called Kummer surfaces.

Question 1 *Does there exist a K3 surface X over a number field K such that the set $X(K)$ of K-rational points on X is neither empty nor dense?*

A few more definitions

The *Néron-Severi group* NS(X) of a surface X is the group of divisor classes modulo algebraic equivalence.

As linear equivalence implies algebraic equivalence, the Néron-Severi group NS(X) of a surface X is a quotient of the Picard group Pic X.

For a K3 surface linear and algebraic equivalence are equivalent, so we get an isomorphism Pic $X \cong$ NS(X).

The Néron-Severi group of a surface X over a field K is a finitely generated abelian group. The *Picard number* $\rho(X)$ of X is defined to be the rank of this group. The Picard number of $\overline{X} = X \times_K \overline{K}$ is called the *geometric Picard number* of X.

Inequalities

We have $1 \leq \rho(X) \leq \rho(\overline{X})$. The first inequality comes from the existence of a hyperplane section, the second from the injection

$$\mathrm{NS}(X) \hookrightarrow \mathrm{NS}(\overline{X}).$$

The Néron-Severi group $\mathrm{NS}(\overline{X})$ injects into an H^2, so we also have $\rho(\overline{X}) \leq b_2$, where b_2 is the second betti number. For K3 surfaces we get

$$1 \leq \rho(X) \leq \rho(\overline{X}) \leq 22.$$

Let X be a quartic surface in $\mathbb{P}^3$.
Then the following are equivalent.

(a) X has Picard number 1.

(b) Every curve on X is equal to the complete intersection of X with a hypersurface.

Let X be a quartic surface in $\mathbb{P}^3$.
Then the following are equivalent.

(a) X has Picard number 1.

(b) Every curve on X is equal to the complete intersection of X with a hypersurface.

Vague idea:

The higher the Picard number of X, the "easier" it is for X to have lots of rational points.

Let X be a K3 surface over a number field K. If there exists a finite field extension K'/K such that $X(K')$ is Zariski dense in X, then we say that the rational points on X are *potentially dense*.

Let X be a K3 surface over a number field K. If there exists a finite field extension K'/K such that $X(K')$ is Zariski dense in X, then we say that the rational points on X are *potentially dense*.

Theorem [F. Bogomolov – Y. Tschinkel] Let X be a K3 surface over a Number field. If either

(a) $\rho(\overline{X}) = 2$ and $\overline{X}$ does not contain a (-2)-curve, or

(b) $\rho(\overline{X}) \geq 3$ (except for 8 isomorphism classes of $\mathrm{Pic}\,\overline{X}$),

then the rational points on X are potentially dense.

Let X be a K3 surface over a number field K. If there exists a finite field extension K'/K such that $X(K')$ is Zariski dense in X, then we say that the rational points on X are *potentially dense*.

Theorem [F. Bogomolov – Y. Tschinkel] Let X be a K3 surface over a Number field. If either

(a) $\rho(\overline{X}) = 2$ and $\overline{X}$ does not contain a (-2)-curve, or

(b) $\rho(\overline{X}) \geq 3$ (except for 8 isomorphism classes of $\operatorname{Pic}\overline{X}$),

then the rational points on X are potentially dense.

Question 2 *Is there a K3 surface X over a number field with $\rho(\overline{X}) = 1$ on which the rational points are potentially dense?*

Let X be a K3 surface over a number field K. If there exists a finite field extension K'/K such that $X(K')$ is Zariski dense in X, then we say that the rational points on X are *potentially dense*.

Theorem [F. Bogomolov – Y. Tschinkel] Let X be a K3 surface over a Number field. If either

(a) $\rho(\overline{X}) = 2$ and $\overline{X}$ does not contain a (-2)-curve, or

(b) $\rho(\overline{X}) \geq 3$ (except for 8 isomorphism classes of $\operatorname{Pic} \overline{X}$),

then the rational points on X are potentially dense.

Question 2 *Is there a K3 surface X over a number field with $\rho(\overline{X}) = 1$ on which the rational points are potentially dense?*

Question 3 *Is there a K3 surface X over a number field with $\rho(\overline{X}) = 1$ on which the rational points are* **not** *potentially dense?*

At the AIM conference on rational and integral points on higher-dimensional varieties in December 2002, Sir P. Swinnerton-Dyer posed the following easier variation of these questions.

Question 4 *Is there a K3 surface over a number field with Picard number* 1 *on which there are infinitely many rational points?*

We will see that they do exist, even with the *geometric* Picard number equal to 1. We can also take the ground field to be $\mathbb{Q}$.

Question 4 *Is there a K3 surface over a number field with Picard number* 1 *on which there are infinitely many rational points?*

Of the two aspects

"having infinitely many rational points"

and

"having geometric Picard number 1,"

the latter appears to be the harder question, even though Deligne has proved in 1973 that a general quartic surface in $\mathbb{P}^3$ has geometric Picard number 1.

The quartic surfaces in $\mathbb{P}^3$ are parametrized by elements of $\mathbb{P}^{34}$ and "general" means "up to a countable union of proper closed subsets of $\mathbb{P}^{34}$".

A priori this could exclude all quartic surfaces defined over $\overline{\mathbb{Q}}$!

What was known?

Theorem [T. Terasoma, 1985] For given numbers $(2n; a_1, \ldots, a_d)$ not equal to $(2;3)$, $(2n;2)$ and $(2n;2,2)$, there is a smooth complete intersection X over $\mathbb{Q}$ of dimension $2n$ defined by equations of degrees $a_1, \cdots, a_d$ such that the middle geometric Picard number of X is 1.

Theorem [J. Ellenberg, 2004] For every even integer d there exists a number field K and a polarized K3 surface X/K, of degree d, with $\rho(\overline{X}) = 1$.

Explicit constructive result

Theorem [T. Shioda] For every prime $m \geq 5$ the surface in $\mathbb{P}^3$ given by

$$w^m + xy^{m-1} + yz^{m-1} + zx^{m-1} = 0$$

has geometric Picard number 1.

The challenge to find an *explicit* K3 surface with geometric Picard number 1 has been around for at least 25 years. The challenge has been attributed to D. Mumford.

Theorem The quartic surface in $\mathbb{P}^3(x, y, z, w)$ given by

$$wf = 3pq - 2zg$$

with $f \in \mathbb{Z}[x, y, z, w]$ and $g, p, q \in \mathbb{Z}[x, y, z]$ equal to

$$\begin{aligned} f = {} & x^3 - x^2y - x^2z + x^2w - xy^2 - xyz + 2xyw + xz^2 + 2xzw + y^3 \\ & + y^2z - y^2w + yz^2 + yzw - yw^2 + z^2w + zw^2 + 2w^3, \\ g = {} & xy^2 + xyz - xz^2 - yz^2 + z^3, \\ p = {} & z^2 + xy + yz, \\ q = {} & z^2 + xy \end{aligned}$$

has geometric Picard number 1 and infinitely many rational points.

Theorem The quartic surface S in $\mathbb{P}^3(x, y, z, w)$ given by

$$wf = 3pq - 2zg$$

with [...] has geometric Picard number 1 and infinitely many rational points.

There are infinitely many rational points in the intersection C of S with the plane H_w given by $w = 0$. This does not contradict Faltings' Theorem because the plane H_w is tangent to S at two points, namely $[1 : 0 : 0 : 0]$ and $[0 : 1 : 0 : 0]$. Therefore, the intersection C has geometric genus at most 1 instead of 3, and it turns out that C is an elliptic curve with infinitely many rational points.

This was not just lucky as the construction yields rank 2 generically.

Bounding the Picard number from above

Let X be a (smooth, projective, geometrically integral) surface over $\mathbb{Q}$ and let $\mathcal{X}$ be an integral model of X with good reduction at the prime p.

From étale cohomology we get injections

$$\mathrm{NS}(X_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}_l \hookrightarrow \mathrm{NS}(\mathcal{X}_{\overline{\mathbb{F}_p}}) \otimes \mathbb{Q}_l \hookrightarrow H^2_{\text{ét}}(\mathcal{X}_{\overline{\mathbb{F}_p}}, \mathbb{Q}_l)(1).$$

The second injection respects Frobenius.

Corollary The rank $\rho(X_{\overline{\mathbb{Q}}})$ is bounded from above by the number of eigenvalues λ of Frobenius acting on $H^2_{\text{ét}}(\mathcal{X}_{\overline{\mathbb{F}_p}}, \mathbb{Q}_l)(1)$ for which λ is a root of unity.

$$\mathsf{NS}(X_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}_l \hookrightarrow \mathsf{NS}(\mathcal{X}_{\overline{\mathbb{F}_p}}) \otimes \mathbb{Q}_l \hookrightarrow H^2_{\text{ét}}(\mathcal{X}_{\overline{\mathbb{F}_p}}, \mathbb{Q}_l)(1).$$

The geometric Frobenius φ acting on $H^2_{\text{ét}}(\mathcal{X}_{\overline{\mathbb{F}_p}}, \mathbb{Q}_l)$ (without the Tate twist) has exactly the same eigenvalues, except multiplied by p. This is exactly the Frobenius that comes up in the Weil conjectures and the Lefschetz formula.

We can compute the characteristic polynomial of φ by computing traces of powers of φ through the Lefschetz formula

$$\#\mathcal{X}(\mathbb{F}_{p^n}) = \sum_{i=0}^{4} (-1)^i \,\mathrm{Tr}(n\text{-th power of Frobenius on } H^i_{\text{ét}}(\mathcal{X}_{\overline{\mathbb{F}_p}}, \mathbb{Q}_l)).$$

$$\#\mathcal{X}(\mathbb{F}_{p^n}) = \sum_{i=0}^{4} (-1)^i \,\text{Tr}(n\text{-th power of Frobenius on } H^i_{\text{ét}}(\mathcal{X}_{\overline{\mathbb{F}_p}}, \mathbb{Q}_l)).$$

Knowing traces, the characteristic polynomial follows:

Lemma V a vector space, $\dim V = n$, and T acts linearly on V. Let $t_i = \text{Tr}\, T^i$. Then characteristic polynomial of T is

$$f_T(x) = \det(x \cdot \text{Id} - T) = x^n + c_1 x^{n-1} + c_2 x^{n-2} + \ldots + c_n,$$

with the c_i given recursively by

$$c_1 = -t_1 \text{ and } -kc_k = t_k + \sum_{i=1}^{k-1} c_i t_{k-i}.$$

Scaling $x \mapsto px$ gives characteristic polynomial on $H^i_{\text{ét}}(\mathcal{X}_{\overline{\mathbb{F}_p}}, \mathbb{Q}_l)(1)$.

Problem!

Lemma Let f be a polynomial with real coefficients and even degree, such that all its roots have complex absolute value 1. Then the number of roots of f that are roots of unity is even.

Proof. All the real roots of f are roots of unity. The remaining roots come in conjugate pairs, either both being a root of unity or both not being a root of unity.

Problem!

Lemma Let f be a polynomial with real coefficients and even degree, such that all its roots have complex absolute value 1. Then the number of roots of f that are roots of unity is even.

Proof. All the real roots of f are roots of unity. The remaining roots come in conjugate pairs, either both being a root of unity or both not being a root of unity.

Because Tate's conjecture says that the Néron-Severi rank of the reduction is actually equal to this upper bound, it will not be good enough to just look at the reduction modulo a prime of good reduction if we want to get upper bound 1.

An idea from elliptic curves

Let E be an elliptic curve over $\mathbb{Q}$. Let $\tilde{E}_p$ be the reduction of an integral model of E at a prime p of good reduction. Then the torsion subgroup of $E(\mathbb{Q})$ injects into the torsion of $\tilde{E}_p(\mathbb{F}_p)$.

Therefore, $\#E(\mathbb{Q})_{\text{tors}}$ is a divisor of $N_p = \#\tilde{E}_p(\mathbb{F}_p)$. This could help to find the torsion subgroup of $E(\mathbb{Q})$, but sometimes N_p is a multiple of 4 for every p even though $\#E(\mathbb{Q})_{\text{tors}}$ is not.

We can get more information by looking at the group structure of the reduction for various primes. By looking at the 2-part of $\tilde{E}_p(\mathbb{F}_p)$ one might find that for some p it is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ and for other p to $(\mathbb{Z}/2\mathbb{Z})^2$. Then $\#E(\mathbb{Q})_{\text{tors}} \leq 2$.

Where were we going?

Theorem The quartic surface S in $\mathbb{P}^3_{\mathbb{Z}}(x,y,z,w)$ given by

$$wf = 3pq - 2zg$$

with $f \in \mathbb{Z}[x,y,z,w]$ and $g,p,q \in \mathbb{Z}[x,y,z]$ equal to

$$\begin{aligned} f = {} & x^3 - x^2y - x^2z + x^2w - xy^2 - xyz + 2xyw + xz^2 + 2xzw + y^3 \\ & + y^2z - y^2w + yz^2 + yzw - yw^2 + z^2w + zw^2 + 2w^3, \\ g = {} & xy^2 + xyz - xz^2 - yz^2 + z^3, \\ p = {} & z^2 + xy + yz, \\ q = {} & z^2 + xy \end{aligned}$$

has geometric Picard number 1 and infinitely many rational points.

Similar to the elliptic curves, we will prove that our S has geometric Picard number 1 by reducing it modulo the primes of good reduction 2 and 3 and combining the local information.

A little more theory

A *lattice* is a free $\mathbb{Z}$-module Λ of finite rank, together with a symmetric nondegenerate bilinear pairing $\Lambda \times \Lambda \to \mathbb{Q}$. A *sublattice* of Λ is a submodule Λ' of Λ such that the induced bilinear pairing on Λ' is nondegenerate.

The discriminant of a lattice Λ is the determinant of the Gram matrix (w.r.t. any basis) that gives the inner product on Λ.

Lemma If Λ' is a sublattice of finite index of Λ, then we have

$$\operatorname{disc} \Lambda' = [\Lambda : \Lambda']^2 \operatorname{disc} \Lambda.$$

This implies that $\operatorname{disc} \Lambda$ and $\operatorname{disc} \Lambda'$ have the same image in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.

The intersection pairing gives the Néron-Severi group the structure of a *lattice*.

The injection

$$\mathrm{NS}(X_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}_l \hookrightarrow \mathrm{NS}(\mathcal{X}_{\overline{\mathbb{F}_p}}) \otimes \mathbb{Q}_l$$

of $\mathbb{Q}_l$-vector spaces respects the inner product.

Sketch of proof

The main argument will be that we can find finite index sublattices M_2 and M_3 of the Néron-Severi groups over $\overline{\mathbb{F}_2}$ and $\overline{\mathbb{F}_3}$ respectively. Both will have rank 2, which already shows that the rank of $\mathrm{NS}(S_{\overline{\mathbb{Q}}})$ is at most 2. We get the following diagram

$$\begin{array}{ccccc} \mathrm{NS}(S_{\overline{\mathbb{Q}}}) & \subset & \mathrm{NS}(S_{\overline{\mathbb{F}_2}}) & \supset & M_2 \\ \| & & & & \\ \mathrm{NS}(S_{\overline{\mathbb{Q}}}) & \subset & \mathrm{NS}(S_{\overline{\mathbb{F}_3}}) & \supset & M_3 \end{array}$$

The images of $\operatorname{disc} M_2$ and $\operatorname{disc} M_3$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ will be different, so $\mathrm{NS}(S_{\overline{\mathbb{Q}}})$ has rank at most 1.

The example

$$wf = 3pq - 2zg$$

was constructed in such a way that modulo 2 and 3 we can a priori account for a rank 2 part of the Néron-Severi lattice.

After reduction modulo 3, the surface S_3 is given by $wf = zg$, for some cubic forms f and g. The surface S_3 therefore contains a line L given by $w = z = 0$. By the adjunction formula

$$L \cdot (L + K_{S_3}) = 2g(L) - 2 = -2,$$

where $K_{S_3} = 0$ is a canonical divisor on S_3, we find $L^2 = -2$. Let M_3 be the lattice generated by the hyperplane section H and L. With respect to $\{H, L\}$ the inner product on M_3 is given by

$$\begin{pmatrix} 4 & 1 \\ 1 & -2 \end{pmatrix}.$$

With respect to $\{H, L\}$ the inner product on M_3 is given by

$$\begin{pmatrix} 4 & 1 \\ 1 & -2 \end{pmatrix}.$$

We get $\operatorname{disc} M_3 = -9$. By counting points as described before we find that the characteristic polynomial of Frobenius acting on $H^2_{\text{ét}}(S_{\overline{\mathbb{F}_3}}, \mathbb{Q}_l)(1)$ factors over $\mathbb{Q}$ as

$$\begin{aligned}(x-1)^2(x^{20} &+ \tfrac{1}{3}x^{19} - x^{18} + \tfrac{1}{3}x^{17} + 2x^{16} - 2x^{14} + \tfrac{1}{3}x^{13} \\ &+ 2x^{12} - \tfrac{1}{3}x^{11} - \tfrac{7}{3}x^{10} - \tfrac{1}{3}x^9 + 2x^8 + \tfrac{1}{3}x^7 - 2x^6 \\ &+ 2x^4 + \tfrac{1}{3}x^3 - x^2 + \tfrac{1}{3}x + 1).\end{aligned}$$

As the second factor is not integral, we find that exactly 2 of its roots are roots of unity. We conclude that M_3 has finite index in $\mathrm{NS}(S_{\overline{\mathbb{F}_3}})$.

The example is still

$$wf = 3pq - 2zg.$$

After reduction modulo 2, the surface S_2 is given by $wf = pq$, for some quadratic forms p and q. The surface S_2 therefore contains a conic C given by $w = p = 0$. By the adjunction formula

$$C \cdot (C + K_{S_2}) = 2g(C) - 2 = -2,$$

we find $C^2 = -2$. Let M_2 be the lattice generated by the hyperplane section H and C. With respect to $\{H, C\}$ the inner product on M_3 is given by

$$\begin{pmatrix} 4 & 2 \\ 2 & -2 \end{pmatrix}.$$

With respect to $\{H, C\}$ the inner product on M_2 is given by

$$\begin{pmatrix} 4 & 2 \\ 2 & -2 \end{pmatrix}.$$

We get $\operatorname{disc} M_2 = -12$. By counting points as described before we find that the characteristic polynomial of Frobenius acting on $H^2_{\text{ét}}(S_{\overline{\mathbb{F}_2}}, \mathbb{Q}_l)(1)$ factors over $\mathbb{Q}$ as

$$(x-1)^2(x^{20} + \tfrac{1}{2}x^{19} - \tfrac{1}{2}x^{18} + \tfrac{1}{2}x^{16} + \tfrac{1}{2}x^{14} + \tfrac{1}{2}x^{11} + x^{10} + \tfrac{1}{2}x^9 + \tfrac{1}{2}x^6 + \tfrac{1}{2}x^4 - \tfrac{1}{2}x^2 + \tfrac{1}{2}x + 1).$$

The last factor is not integral, so M_2 has finite index in $\mathrm{NS}(S_{\overline{\mathbb{F}_2}})$.

As $\operatorname{disc} M_3 = -9$ and $\operatorname{disc} M_2 = -12$ do not have the same image in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, we have proven that $\mathrm{NS}(S_{\overline{\mathbb{Q}}})$ has rank 1. By the adjunction formula the lattice is even, so it is generated by H.

A slight variation of the argument (working over $\mathbb{F}_4$ instead of $\mathbb{F}_2$) shows

Theorem The nonsingular quartic K3 surface in $\mathbb{P}^3$ given by

$$w(x^3+y^3+z^3+x^2z+xw^2) = 3x^2y^2-4x^2yz+x^2z^2+xy^2z+xyz^2-y^2z^2$$

has geometric Picard number 1. The hyperplane section given by $w = 0$ can be parametrized by

$$\left(\frac{y}{x}, \frac{z}{x}\right) = \left(-\frac{2(t+2)}{t^2-t-3}, -\frac{2(t+2)}{t^2+t-1}\right).$$

Problem with this method to find Picard numbers:

One needs to know generators of a finite index subgroup of the Néron-Severi group modulo two different primes p to compute the discriminant up to squares.

Problem with this method to find Picard numbers:

One needs to know generators of a finite index subgroup of the Néron-Severi group modulo two different primes p to compute the discriminant up to squares.

Solution [R. Kloosterman]

For elliptic K3 surfaces the Brauer group has square order. The Artin-Tate conjectures then allow us to compute

$$\operatorname{disc} \mathrm{NS}(S) \mod {\mathbb{Q}^*}^2$$

from the characteristic polynomial of Frobenius.

Theorem [R. Kloosterman] The minimal nonsingular model of the surface given by

$$y^2 = x^3 + 2(t^8 + 14t^4 + 1)x + 4t^2(t^8 + 6t^4 + 1)$$

is an elliptic K3 surface of Néron-Severi rank 17. The Mordell-Weil rank of the generic fiber equals 15, the only missing value in a list of Kuwata.

Questure:

Let X be a K3 surface over a number field k with rank NS($X_{\overline{k}}$) = 1. Is there a finite field extension l, a constant C, and an open subset $U \subset X$, such that U contains no curve of genus 1 over l and

$$\#\{x \in U(l) \ : \ H(x) \leq B\} \ \approx \ C \log B?$$