Geometry dictates arithmetic

Ronald van Luijk

February 21, 2013
Utrecht

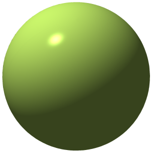
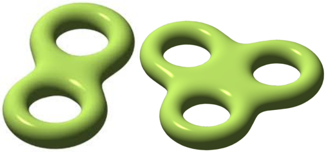
Curves

Example. Circle given by $x^2 + y^2 = 1$ (or projective closure in $\mathbb{P}^2$).

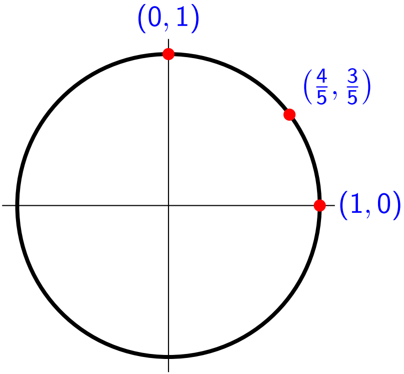
Curves

Example. Circle given by $x^2 + y^2 = 1$ (or projective closure in $\mathbb{P}^2$).

Definition.
Genus of a smooth projective curve C over $\mathbb{Q}$ is the genus of $C(\mathbb{C})$.

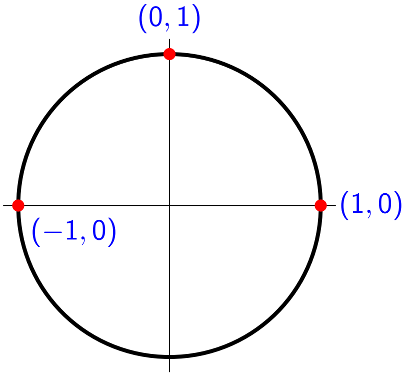
$g = 0$	$g = 1$	$g \geq 2$
		

Genus 0



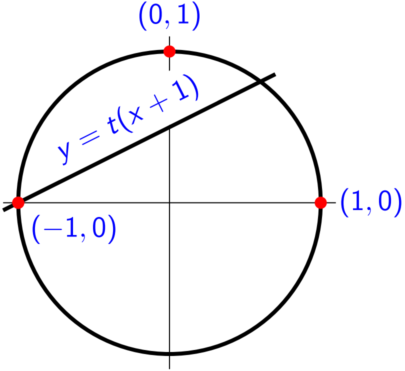
$\mathbb{P}^2 \supset C : x^2 + y^2 = 1$

Genus 0



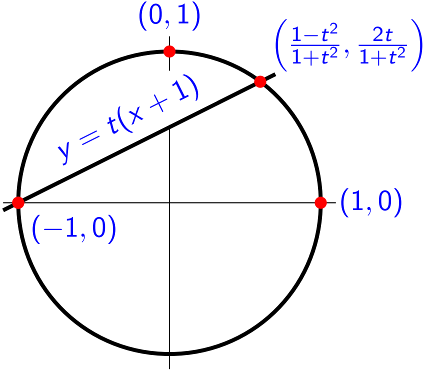
$\mathbb{P}^2 \supset C\colon x^2 + y^2 = 1$

Genus 0



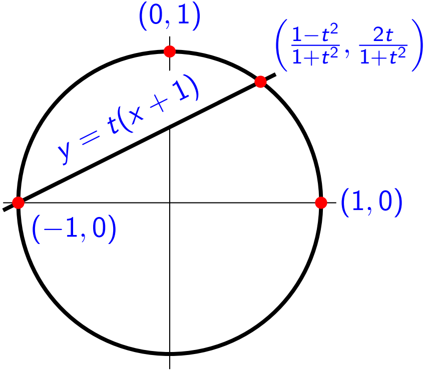
$\mathbb{P}^2 \supset C \colon x^2 + y^2 = 1$

Genus 0



$\mathbb{P}^2 \supset C\colon x^2 + y^2 = 1$

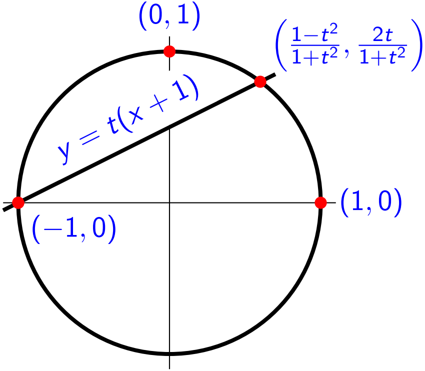
Genus 0



$\mathbb{P}^2 \supset C\colon x^2 + y^2 = 1$

Theorem. If a conic over $\mathbb{Q}$ has a rational point, then it has infinitely many.

Genus 0

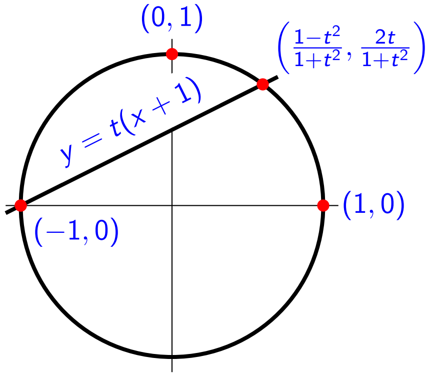


$\mathbb{P}^2 \supset C\colon x^2 + y^2 = 1$

Theorem. If a conic over $\mathbb{Q}$ has a rational point, then it has infinitely many.

Theorem. If a conic D over $\mathbb{Q}$ has a rational point, then there is an isomorphism $\mathbb{P}^1(\mathbb{C}) \to D(\mathbb{C})$, so the genus of D is 0.

Genus 0



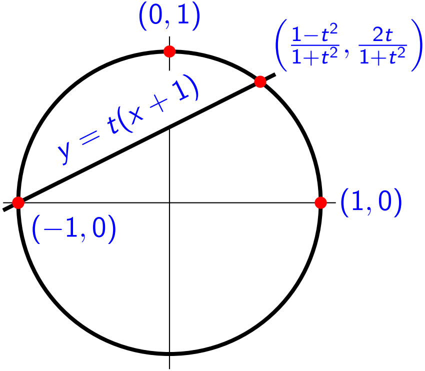
$\mathbb{P}^2 \supset C\colon x^2 + y^2 = 1$

Theorem. If a conic over $\mathbb{Q}$ has a rational point, then it has infinitely many.

Theorem. If a conic D over $\mathbb{Q}$ has a rational point, then there is an isomorphism $\mathbb{P}^1(\mathbb{C}) \to D(\mathbb{C})$, so the genus of D is 0.

Theorem. Any curve of genus 0 over $\mathbb{Q}$ is isomorphic to a conic.

Genus 0



$\mathbb{P}^2 \supset C\colon x^2 + y^2 = 1$

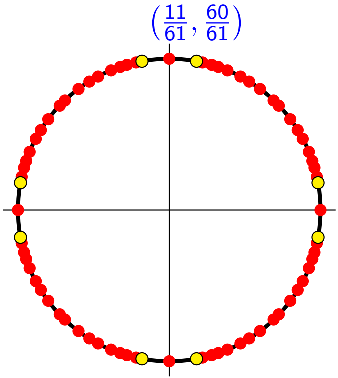
Theorem. If a conic over $\mathbb{Q}$ has a rational point, then it has infinitely many.

Theorem. If a conic D over $\mathbb{Q}$ has a rational point, then there is an isomorphism $\mathbb{P}^1(\mathbb{C}) \to D(\mathbb{C})$, so the genus of D is 0.

Theorem. Any curve of genus 0 over $\mathbb{Q}$ is isomorphic to a conic.

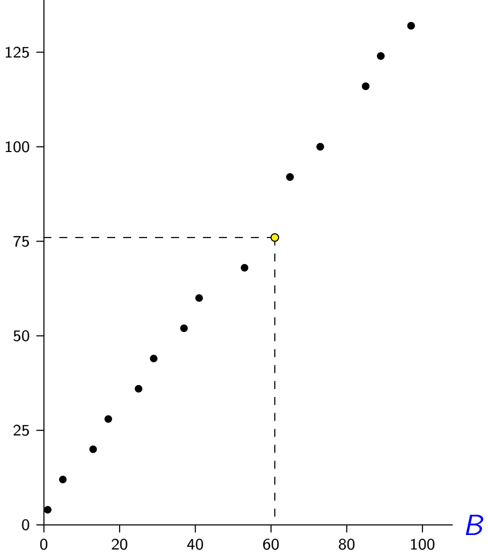
Theorem. If a curve of genus 0 over $\mathbb{Q}$ has a rational point, then it is isomorphic to $\mathbb{P}^1$ and it has infinitely many rational points.

Genus 0

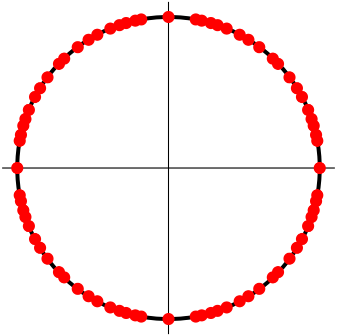


$\mathbb{P}^2 \supset C\colon x^2 + y^2 = 1$

$N_C(B) =$
number of $\left(\frac{a}{c}, \frac{b}{c}\right)$
with $|a|, |b|, |c| \leq B$

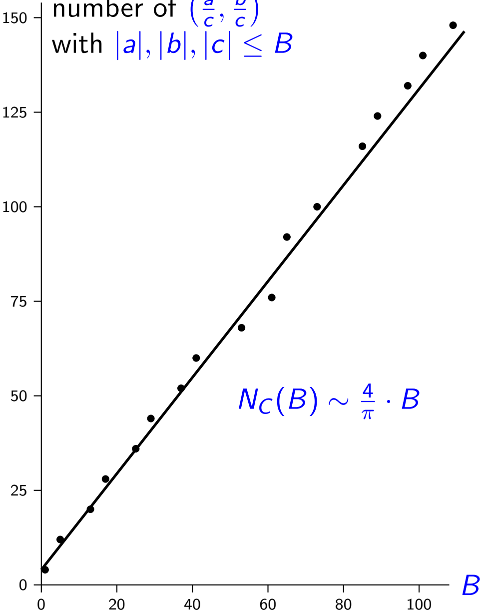


Genus 0



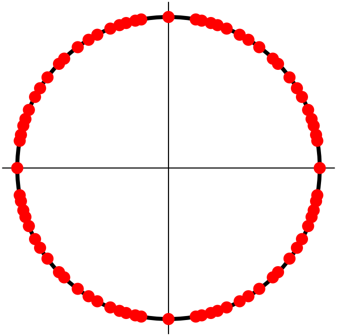
$\mathbb{P}^2 \supset C\colon x^2 + y^2 = 1$

$N_C(B) =$
number of $\left(\frac{a}{c}, \frac{b}{c}\right)$
with $|a|, |b|, |c| \le B$

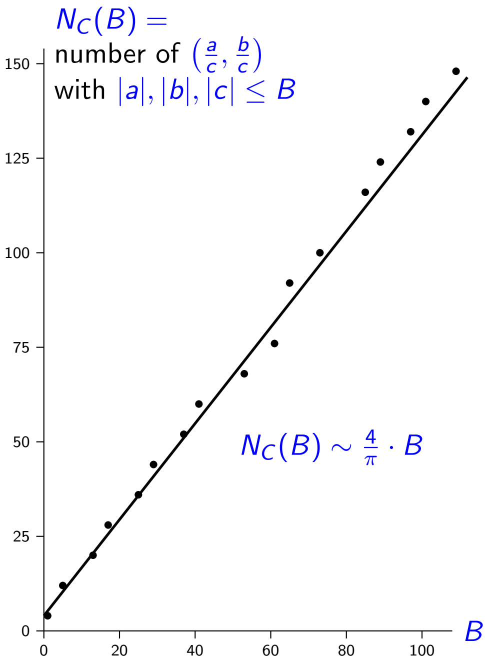


$N_C(B) \sim \frac{4}{\pi} \cdot B$

Genus 0

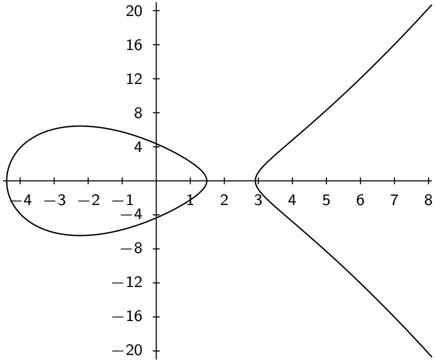


$\mathbb{P}^2 \supset C\colon x^2 + y^2 = 1$

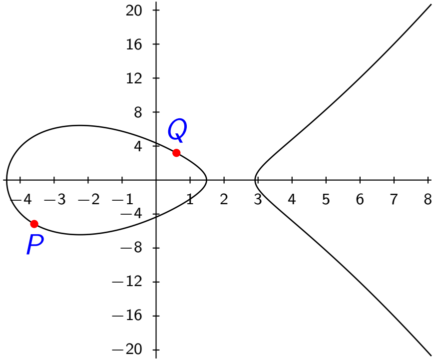


Theorem. The number $N_D(B)$ of rational points on a conic D grows linearly with the height B (or is zero).

Genus 1 (elliptic)

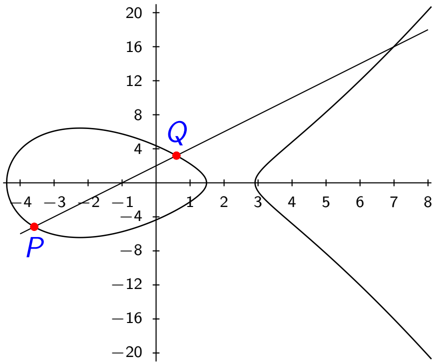


Genus 1 (elliptic)



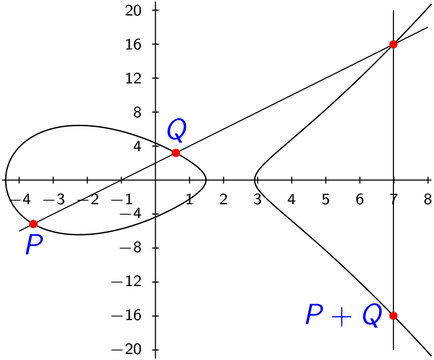
$$E\colon y^2 = x^3 - 15x + 19$$

Genus 1 (elliptic)



$E\colon y^2 = x^3 - 15x + 19$

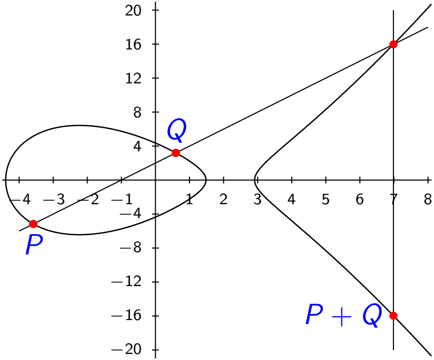
Genus 1 (elliptic)



$E\colon y^2 = x^3 - 15x + 19$

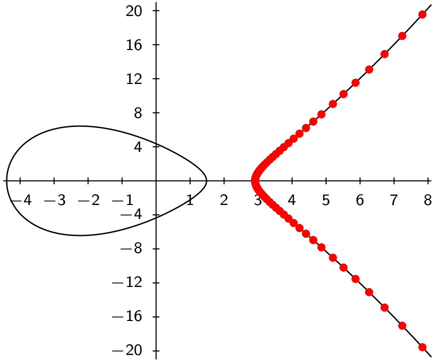
Genus 1 (elliptic)

Fact. $E(k)$ is an abelian group!



$E \colon y^2 = x^3 - 15x + 19$

Genus 1 (elliptic)



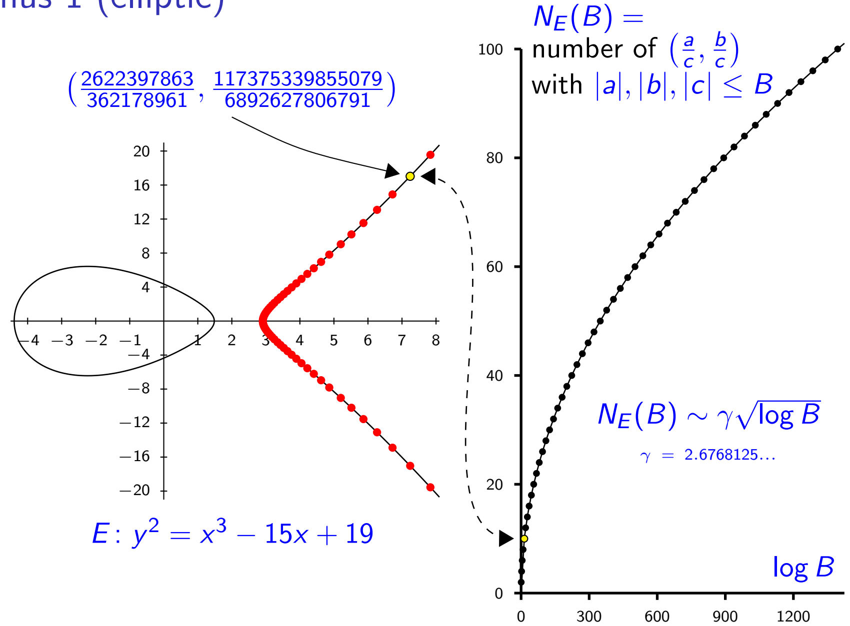
$E\colon y^2 = x^3 - 15x + 19$

Fact. $E(k)$ is an abelian group!

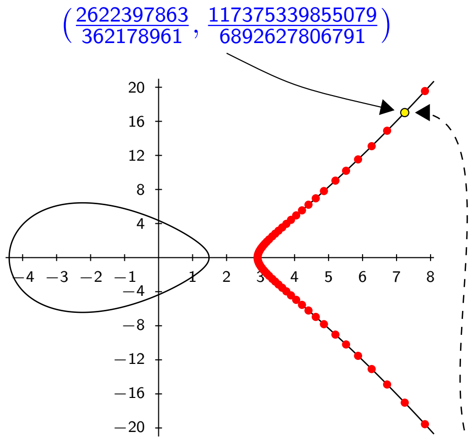
Theorem (Mordell-Weil).
For any elliptic curve E over $\mathbb{Q}$, the group $E(\mathbb{Q})$ is finitely generated.

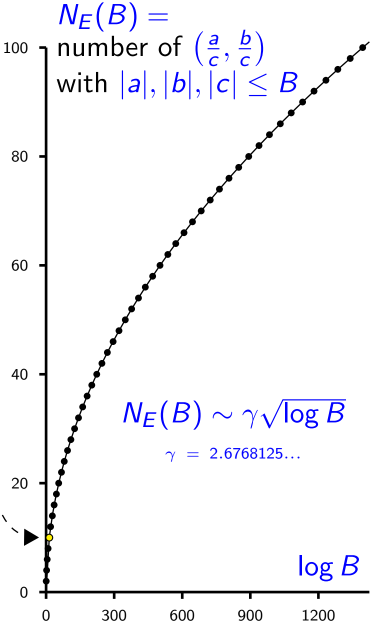
Here: rank$=1$, and
$\mathbb{Z} \cong E(\mathbb{Q}) = \langle (3,1) \rangle$.

Genus 1 (elliptic)



Genus 1 (elliptic)





Theorem. For any elliptic curve E over $\mathbb{Q}$ with $r = \operatorname{rank} E(\mathbb{Q})$, we have $N_E(B) \sim c(\log B)^{r/2}$.

Genus $g \geq 2$

Examples.

- $y^2 = f(x)$ with f separable of degree $2g + 2$.
- smooth projective plane curve of degree $d \geq 4$ with $g = \frac{1}{2}(d-1)(d-2)$.

Genus $g \geq 2$

Examples.

- $y^2 = f(x)$ with f separable of degree $2g + 2$.
- smooth projective plane curve of degree $d \geq 4$ with $g = \frac{1}{2}(d-1)(d-2)$.

Theorem ("Mordell Conjecture" by Faltings, 1983).
Any curve over $\mathbb{Q}$ with $g \geq 2$ has only finitely many rational points.

Genus $g \geq 2$

Examples.

- $y^2 = f(x)$ with f separable of degree $2g + 2$.
- smooth projective plane curve of degree $d \geq 4$ with $g = \frac{1}{2}(d-1)(d-2)$.

Theorem ("Mordell Conjecture" by Faltings, 1983).
Any curve over $\mathbb{Q}$ with $g \geq 2$ has only finitely many rational points.

Conclusion.
"The higher the genus, the lower the number of rational points".

Differentials

Definition.
Let X be a smooth projective variety with function field $k(X)$.
Then $\Omega_{k(X)/k}$ is the $k(X)$-vectorspace of differential 1-forms, generated by $\{df : f \in k(X)\}$ and satisfying

- $d(f+g) = df + dg$,
- $d(fg) = fdg + gdf$,
- $da = 0$ for $a \in k$.

Differentials

Definition.
Let X be a smooth projective variety with function field $k(X)$.
Then $\Omega_{k(X)/k}$ is the $k(X)$-vectorspace of differential 1-forms, generated by $\{df : f \in k(X)\}$ and satisfying

- $d(f+g) = df + dg$,
- $d(fg) = fdg + gdf$,
- $da = 0$ for $a \in k$.

Proposition. We have $\dim_{k(X)} \Omega_{k(X)/k} = \dim X$.

Example.
For curve $C\colon y^2 = f(x)$ we have $2ydy = f'(x)dx$ in $\Omega_{k(C)/k}$.

Holomorphic differentials on curves

Definition. For a point P on a smooth projective curve C with local parameter $t_P \in k(C)$ and a differential $\omega \in \Omega_{k(C)/k}$, we write $\omega = f_P dt_P$; then ω is holomorphic at P if f_P has no pole at P.

Example.
Curve $C\colon y^2 = f(x)$ with f separable of degree $d \geq 3$. Then

$$\omega = \frac{1}{y} d(x - c) = \frac{1}{y} dx = \frac{2}{f'(x)} dy$$

is holomorphic **everywhere**.

Holomorphic differentials on curves

Definition. For a point P on a smooth projective curve C with local parameter $t_P \in k(C)$ and a differential $\omega \in \Omega_{k(C)/k}$, we write $\omega = f_P dt_P$; then ω is holomorphic at P if f_P has no pole at P.

Example.
Curve $C\colon y^2 = f(x)$ with f separable of degree $d \geq 3$. Then

$$\omega = \frac{1}{y} d(x-c) = \frac{1}{y} dx = \frac{2}{f'(x)} dy$$

is holomorphic **everywhere**.

Definition. Set $\Omega_{C/k} = \{\omega \in \Omega_{k(C)/k} : \omega \text{ holom. everywhere}\}$.

Proposition. We have $g = \dim_k \Omega_{C/k}$.

Holomorphic differentials in general

Recall. If X smooth, projective, then $\dim_{k(X)} \Omega_{k(X)/k} = \dim X$.

Fact. If V is a vector space with $\dim V = n$, then $\dim \bigwedge^n V = 1$.

Holomorphic differentials in general

Recall. If X smooth, projective, then $\dim_{k(X)} \Omega_{k(X)/k} = \dim X$.

Fact. If V is a vector space with $\dim V = n$, then $\dim \bigwedge^n V = 1$.

Definition (unconventional notation for $(\dim X)$-forms).
Set $\Omega_{X/k} = \{\omega \in \bigwedge^{\dim X} \Omega_{k(X)/k} \;:\; \omega \text{ holom. everywhere}\}$.

Holomorphic differentials in general

Recall. If X smooth, projective, then $\dim_{k(X)} \Omega_{k(X)/k} = \dim X$.

Fact. If V is a vector space with $\dim V = n$, then $\dim \bigwedge^n V = 1$.

Definition (unconventional notation for $(\dim X)$-forms).
Set $\Omega_{X/k} = \{\omega \in \bigwedge^{\dim X} \Omega_{k(X)/k} \ : \ \omega \text{ holom. everywhere}\}$.

Definition
For a k-basis $(\omega_0, \omega_1, \ldots, \omega_N)$ of $\Omega_{X/k}$, we get $f_i \in k(X)$ such that $\omega_i = f_i \omega_0$. The Kodaira dimension $\kappa(X)$ of X is -1 if $\dim_k \Omega_{X/k} = 0$, or the dimension of the image of the map

$$X \to \mathbb{A}^N, \qquad P \mapsto (f_1(P), f_2(P), \ldots, f_N(P)).$$

Holomorphic differentials in general

Recall. If X smooth, projective, then $\dim_{k(X)} \Omega_{k(X)/k} = \dim X$.

Fact. If V is a vector space with $\dim V = n$, then $\dim \bigwedge^n V = 1$.

Definition (unconventional notation for $(\dim X)$-forms).
Set $\Omega_{X/k} = \{\omega \in \bigwedge^{\dim X} \Omega_{k(X)/k} \ : \ \omega \text{ holom. everywhere}\}$.

Definition (Wrong: use tensor powers of $\bigwedge^{\dim X} \Omega_{k(X)/k}$.)
For a k-basis $(\omega_0, \omega_1, \ldots, \omega_N)$ of $\Omega_{X/k}$, we get $f_i \in k(X)$ such that $\omega_i = f_i \omega_0$. The Kodaira dimension $\kappa(X)$ of X is -1 if $\dim_k \Omega_{X/k} = 0$, or the dimension of the image of the map

$$X \to \mathbb{A}^N, \qquad P \mapsto (f_1(P), f_2(P), \ldots, f_N(P)).$$

Holomorphic differentials in general

Recall. If X smooth, projective, then $\dim_{k(X)} \Omega_{k(X)/k} = \dim X$.

Fact. If V is a vector space with $\dim V = n$, then $\dim \bigwedge^n V = 1$.

Definition (unconventional notation for $(\dim X)$-forms).
Set $\Omega_{X/k} = \{\omega \in \bigwedge^{\dim X} \Omega_{k(X)/k} \;:\; \omega \text{ holom. everywhere}\}$.

Definition (Wrong: use tensor powers of $\bigwedge^{\dim X} \Omega_{k(X)/k}$.)
For a k-basis $(\omega_0, \omega_1, \dots, \omega_N)$ of $\Omega_{X/k}$, we get $f_i \in k(X)$ such that $\omega_i = f_i \omega_0$. The Kodaira dimension $\kappa(X)$ of X is -1 if $\dim_k \Omega_{X/k} = 0$, or the dimension of the image of the map

$$X \to \mathbb{A}^N, \qquad P \mapsto (f_1(P), f_2(P), \dots, f_N(P)).$$

Proposition. For a curve C we get

$$\kappa(C) = \begin{cases} -1 & g = 0 \\ 0 & g = 1 \\ 1 & g \geq 2 \end{cases}$$

Varieties of general type

In general, $-1 \leq \kappa(X) \leq \dim X$ (complex X $\Rightarrow$ high $\kappa(X)$).

Definition. We say that X is of general type if $\kappa(X) = \dim X$.
("many" holom. differentials, "canonical bundle is pseudo-ample")

Varieties of general type

In general, $-1 \leq \kappa(X) \leq \dim X$ (complex $X \Rightarrow$ high $\kappa(X)$).

Definition. We say that X is of general type if $\kappa(X) = \dim X$.
("many" holom. differentials, "canonical bundle is pseudo-ample")

Conjecture (Lang).
If X is a variety over $\mathbb{Q}$ that is of general type, then the rational points lie in a Zariski closed subset, i.e., a finite union of proper subvarieties of X.

Varieties of general type

In general, $-1 \leq \kappa(X) \leq \dim X$ (complex $X \Rightarrow$ high $\kappa(X)$).

Definition. We say that X is of general type if $\kappa(X) = \dim X$.
("many" holom. differentials, "canonical bundle is pseudo-ample")

Conjecture (Lang).
If X is a variety over $\mathbb{Q}$ that is of general type, then the rational points lie in a Zariski closed subset, i.e., a finite union of proper subvarieties of X.

Corollary. Let $X \subset \mathbb{P}^3$ be a smooth, projective surface over $\mathbb{Q}$ of degree ≥ 5. Then the rational points are all contained in some finite union of curves.

Fano varieties

Definition. A Fano variety is a smooth, projective variety X with ample anti-canonical bundle.

We have $\kappa(X) = -1$ and X is geometrically "easy".

Fano varieties

Definition. A Fano variety is a smooth, projective variety X with ample anti-canonical bundle.

We have $\kappa(X) = -1$ and X is geometrically "easy".

Conjecture (Batyrev-Manin).
Suppose X over $\mathbb{Q}$ is Fano. Set $\rho = \mathrm{rk}\,\mathrm{Pic}\,X$.
There is an open subset $U \subset X$ and a constant c with

$$N_U(B) \sim cB(\log B)^{\rho-1}.$$

Fano varieties

Definition. A Fano variety is a smooth, projective variety X with ample anti-canonical bundle.

We have $\kappa(X) = -1$ and X is geometrically "easy".

Conjecture (Batyrev-Manin).
Suppose X over $\mathbb{Q}$ is Fano. Set $\rho = \mathrm{rk}\,\mathrm{Pic}\,X$.
There is an open subset $U \subset X$ and a constant c with

$$N_U(B) \sim cB(\log B)^{\rho-1}.$$

This is proved in many cases for surfaces.
False in higher dimension, but no counterexamples to lower bound.

Fano varieties

Definition. A Fano variety is a smooth, projective variety X with ample anti-canonical bundle.

We have $\kappa(X) = -1$ and X is geometrically "easy".

Conjecture (Batyrev-Manin).
Suppose X over $\mathbb{Q}$ is Fano. Set $\rho = \mathrm{rk}\,\mathrm{Pic}\,X$.
There is an open subset $U \subset X$ and a constant c with

$$N_U(B) \sim cB(\log B)^{\rho-1}.$$

This is proved in many cases for surfaces.
False in higher dimension, but no counterexamples to lower bound.

Conclusion. The more complex a variety, the fewer rational points.

K3 surfaces

Definition. A K3 surface over $\mathbb{Q}$ is a smooth, projective surface X with $X(\mathbb{C})$ simply connected and with trivial canonical bundle.

There is a unique holomorphic differential and we have $\kappa(X) = 0$.

K3 surfaces

Definition. A K3 surface over $\mathbb{Q}$ is a smooth, projective surface X with $X(\mathbb{C})$ simply connected and with trivial canonical bundle.

There is a unique holomorphic differential and we have $\kappa(X) = 0$.

Examples

- Smooth quartic surfaces in $\mathbb{P}^3$.
- Double cover of $\mathbb{P}^2$ ramified over a smooth sextic.
- Desingularization of $A/\langle[-1]\rangle$ for an abelian surface A.

Theorem (Tschinkel-Bogomolov).
If $\mathrm{rk}\,\mathrm{Pic}\,X \geq 5$, then there is a finite extension K of $\mathbb{Q}$ such that the K-rational points are Zariski dense on X, i.e., rational points are potentially dense on X.

Theorem (Tschinkel-Bogomolov).
If $\operatorname{rk}\operatorname{Pic} X \geq 5$, then there is a finite extension K of $\mathbb{Q}$ such that the K-rational points are Zariski dense on X, i.e., rational points are potentially dense on X.

Question. Is there a K3 surface X over a number field with $\operatorname{rk}\operatorname{Pic} X = 1$ and rational points potentially dense?

Theorem (Tschinkel-Bogomolov).
If $\mathrm{rk}\,\mathrm{Pic}\,X \geq 5$, then there is a finite extension K of $\mathbb{Q}$ such that the K-rational points are Zariski dense on X, i.e., rational points are potentially dense on X.

Question. Is there a K3 surface X over a number field with $\mathrm{rk}\,\mathrm{Pic}\,X = 1$ and rational points potentially dense?

Question. Is there a K3 surface X over a number field with $\mathrm{rk}\,\mathrm{Pic}\,X = 1$ and rational points **not** potentially dense?

Theorem (Tschinkel-Bogomolov).
If $\operatorname{rk}\operatorname{Pic} X \geq 5$, then there is a finite extension K of $\mathbb{Q}$ such that the K-rational points are Zariski dense on X, i.e., rational points are potentially dense on X.

Question. Is there a K3 surface X over a number field with $\operatorname{rk}\operatorname{Pic} X = 1$ and rational points potentially dense?

Question. Is there a K3 surface X over a number field with $\operatorname{rk}\operatorname{Pic} X = 1$ and rational points **not** potentially dense?

Question. Is there a K3 surface X over a number field K with $X(K)$ neither empty nor dense?

K3 surfaces

Theorem (Logan, McKinnon, vL).
Take $a, b, c, d \in \mathbb{Q}^*$ with $abcd \in (\mathbb{Q}^*)^2$. Let $X \subset \mathbb{P}^3$ be given by

$$ax^4 + by^4 + cz^4 + dw^4.$$

If $P \in X(\mathbb{Q})$ has no zero coordinates and P does not lie on one of the 48 lines (no two terms sum to 0), then $X(\mathbb{Q})$ is Zariski dense.

K3 surfaces

Theorem (Logan, McKinnon, vL).
Take $a, b, c, d \in \mathbb{Q}^*$ with $abcd \in (\mathbb{Q}^*)^2$. Let $X \subset \mathbb{P}^3$ be given by

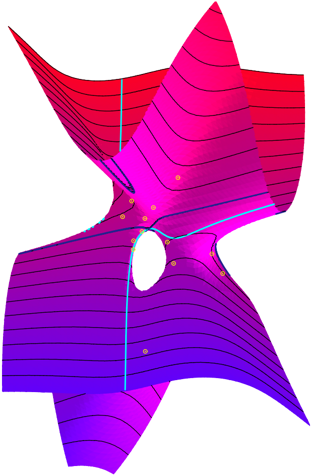
$$ax^4 + by^4 + cz^4 + dw^4.$$

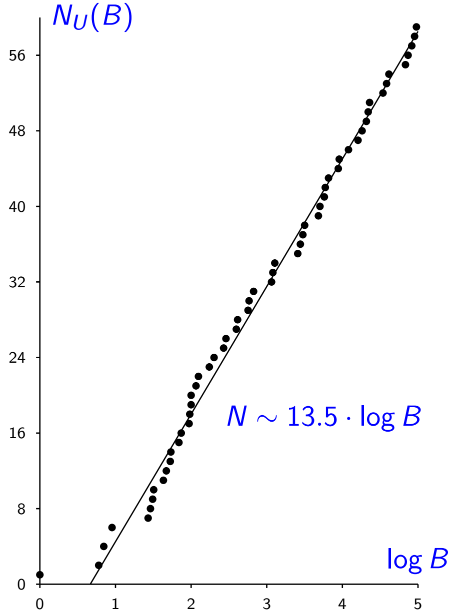
If $P \in X(\mathbb{Q})$ has no zero coordinates and P does not lie on one of the 48 lines (no two terms sum to 0), then $X(\mathbb{Q})$ is Zariski dense.

Question. Are the conditions on P necessary?

Conjecture (vL) Every $t \in \mathbb{Q}$ can be written as

$$t = \frac{x^4 - y^4}{z^4 - w^4}.$$





$$S\colon x^3 - 3x^2y^2 + 4x^2yz - x^2z^2 + x^2z - xy^2z - xyz^2 + x + y^3 + y^2z^2 + z^3 = 0$$

K3 surfaces

Conjecture (vL).
Suppose X is a K3 surface over $\mathbb{Q}$ with $\operatorname{rk}\operatorname{Pic} X_{\mathbb{C}} = 1$.
There is an open subset $U \subset X$ and a constant c such that

$$N_U(B) \sim c \log B.$$

Hasse principle

Theorem (Hasse).
Let $Q \subset \mathbb{P}^n$ be a smooth quadric over $\mathbb{Q}$. Suppose that Q has points over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every p. Then $Q(\mathbb{Q}) \neq \emptyset$.

Hasse principle

Theorem (Hasse).
Let $Q \subset \mathbb{P}^n$ be a smooth quadric over $\mathbb{Q}$. Suppose that Q has points over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every p. Then $Q(\mathbb{Q}) \neq \emptyset$.

Proposition (Selmer).
The curve $C \subset \mathbb{P}^2$ given by $3x^3 + 4y^3 + 5z^3 = 0$ has points over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every p, but $C(\mathbb{Q}) = \emptyset$.

Brauer-Manin obstruction

To every variety X we can assign the Brauer group $\mathrm{Br}\, X$.
Every morphism $X \to Y$ induces a homomorphism $\mathrm{Br}\, Y \to \mathrm{Br}\, X$.
For every point P over a field k we have $\mathrm{Br}(P) = \mathrm{Br}(k)$.

Brauer-Manin obstruction

To every variety X we can assign the Brauer group $\mathrm{Br}\, X$.
Every morphism $X \to Y$ induces a homomorphism $\mathrm{Br}\, Y \to \mathrm{Br}\, X$.
For every point P over a field k we have $\mathrm{Br}(P) = \mathrm{Br}(k)$.

Let X be smooth and projective.

$$
\begin{array}{ccccc}
X(\mathbb{Q}) & \longrightarrow & \prod_v X(\mathbb{Q}_v) & & \\
\downarrow & & \downarrow & \overset{\phi}{\searrow} & \\
\mathrm{Br}(\mathbb{Q}) & \longrightarrow & \bigoplus_v \mathrm{Br}(\mathbb{Q}_v) & \longrightarrow & \mathbb{Q}/\mathbb{Z}
\end{array}
$$

Brauer-Manin obstruction

To every variety X we can assign the Brauer group $\operatorname{Br} X$.
Every morphism $X \to Y$ induces a homomorphism $\operatorname{Br} Y \to \operatorname{Br} X$.
For every point P over a field k we have $\operatorname{Br}(P) = \operatorname{Br}(k)$.

Let X be smooth and projective.

$$\begin{array}{ccccc} X(\mathbb{Q}) & \longrightarrow & \prod_v X(\mathbb{Q}_v) & & \\ \downarrow & & \downarrow & \overset{\phi}{\searrow} & \\ \operatorname{Br}(\mathbb{Q}) & \longrightarrow & \bigoplus_v \operatorname{Br}(\mathbb{Q}_v) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \end{array}$$

Corollary. If $\left(\prod_v X(\mathbb{Q}_v)\right)^{\mathrm{Br}} := \phi^{-1}(0)$ is empty, then $X(\mathbb{Q}) = \emptyset$.

Brauer-Manin obstruction

To every variety X we can assign the Brauer group $\operatorname{Br} X$.
Every morphism $X \to Y$ induces a homomorphism $\operatorname{Br} Y \to \operatorname{Br} X$.
For every point P over a field k we have $\operatorname{Br}(P) = \operatorname{Br}(k)$.

Let X be smooth and projective.

$$
\begin{array}{ccccc}
X(\mathbb{Q}) & \longrightarrow & \prod_v X(\mathbb{Q}_v) & & \\
\downarrow & & \downarrow & \overset{\phi}{\searrow} & \\
\operatorname{Br}(\mathbb{Q}) & \longrightarrow & \bigoplus_v \operatorname{Br}(\mathbb{Q}_v) & \longrightarrow & \mathbb{Q}/\mathbb{Z}
\end{array}
$$

Corollary. If $\left(\prod_v X(\mathbb{Q}_v)\right)^{\operatorname{Br}} := \phi^{-1}(0)$ is empty, then $X(\mathbb{Q}) = \emptyset$.

Conjecture (Colliot-Thélène).
This Brauer-Manin obstruction is the only obstruction to the existence of rational points for rationally connected varieties.