

Local-to-Global obstructions on curves

Nils Bruin

Simon Fraser University

May 13, 2008

Hilbert's Tenth Problem

Hilbert's 10th: Design an automatic procedure that, given a polynomial $f \in \mathbb{Z}[x_1, \dots, x_n]$, decides if

$f(x_1, \dots, x_n) = 0$ has a solution $x_1, \dots, x_n \in \mathbb{Z}$

Hilbert's Tenth Problem

Hilbert's 10th: Design an automatic procedure that, given a polynomial $f \in \mathbb{Z}[x_1, \dots, x_n]$, decides if

$$f(x_1, \dots, x_n) = 0 \text{ has a solution } x_1, \dots, x_n \in \mathbb{Z}$$

Theorem (Davis, Matyasevitch, Putnam, Robinson):
Hilbert's 10th can't be done.

Open questions:

- What if we restrict to a subclass of polynomials?
- What about *rational* solutions rather than *integer* solutions?

Hilbert's Tenth Problem

Hilbert's 10th: Design an automatic procedure that, given a polynomial $f \in \mathbb{Z}[x_1, \dots, x_n]$, decides if

$$f(x_1, \dots, x_n) = 0 \text{ has a solution } x_1, \dots, x_n \in \mathbb{Z}$$

Theorem (Davis, Matyasevitch, Putnam, Robinson):
Hilbert's 10th can't be done.

Open questions:

- What if we restrict to a subclass of polynomials?
- What about *rational* solutions rather than *integer* solutions?

Today: (Smooth) Projective curves over \mathbb{Q} .

Slightly harder: Given $f(x, y) \in \mathbb{Q}[x, y]$, decide if

$$f(x, y) = 0 \text{ has a solution } x, y \in \mathbb{Q}$$

First approaches

Proving a curve does have points: $\mathbb{Q} \times \mathbb{Q}$ is enumerable. Just try candidates until

$$f(x, y) = 0$$

First approaches

Proving a curve does have points: $\mathbb{Q} \times \mathbb{Q}$ is enumerable. Just try candidates until

$$f(x, y) = 0$$

Proving a curve has no points via \mathbb{R} :

$$x^2 + y^2 = -1$$

First approaches

Proving a curve does have points: $\mathbb{Q} \times \mathbb{Q}$ is enumerable. Just try candidates until

$$f(x, y) = 0$$

Proving a curve has no points via \mathbb{R} :

$$x^2 + y^2 = -1$$

Proving a curve has no points via \mathbb{Q}_p :

$$x^2 + y^2 = 3$$

First approaches

Proving a curve does have points: $\mathbb{Q} \times \mathbb{Q}$ is enumerable. Just try candidates until

$$f(x, y) = 0$$

Proving a curve has no points via \mathbb{R} :

$$x^2 + y^2 = -1$$

Proving a curve has no points via \mathbb{Q}_p :

$$x^2 + y^2 = 3 \text{ rewrite as } X^2 + Y^2 = 3Z^2$$

First approaches

Proving a curve does have points: $\mathbb{Q} \times \mathbb{Q}$ is enumerable. Just try candidates until

$$f(x, y) = 0$$

Proving a curve has no points via \mathbb{R} :

$$x^2 + y^2 = -1$$

Proving a curve has no points via \mathbb{Q}_p :

$$x^2 + y^2 = 3 \text{ rewrite as } X^2 + Y^2 = 3Z^2$$

Local obstruction: $C(\mathbb{R})$ or $C(\mathbb{Q}_p)$ is empty.

Proving a curve does have points: $\mathbb{Q} \times \mathbb{Q}$ is enumerable. Just try candidates until

$$f(x, y) = 0$$

Proving a curve has no points via \mathbb{R} :

$$x^2 + y^2 = -1$$

Proving a curve has no points via \mathbb{Q}_p :

$$x^2 + y^2 = 3 \text{ rewrite as } X^2 + Y^2 = 3Z^2$$

Local obstruction: $C(\mathbb{R})$ or $C(\mathbb{Q}_p)$ is empty.

Computability:

- For $k = \mathbb{R}$ or $k = \mathbb{Q}_p$, one can decide if $C(k) = \emptyset$
- For C over \mathbb{Q} one has $C(\mathbb{Q}_p) \neq \emptyset$ for almost all p .

Local-to-Global principle

Question: If $C(\mathbb{Q}_p) \neq \emptyset$ for all p and $C(\mathbb{R}) \neq \emptyset$, does it follow that $C(\mathbb{Q}) \neq \emptyset$?

Hasse-Minkowski: Yes if C is quadratic (genus 0 curves can always be put in quadratic form).

Corollary: Hilbert's 10th for *rational* points on *quadratics* can be solved.

Local-to-Global principle

Question: If $C(\mathbb{Q}_p) \neq \emptyset$ for all p and $C(\mathbb{R}) \neq \emptyset$, does it follow that $C(\mathbb{Q}) \neq \emptyset$?

Hasse-Minkowski: Yes if C is quadratic (genus 0 curves can always be put in quadratic form).

Corollary: Hilbert's 10th for *rational* points on *quadratics* can be solved.

In general: No. Selmer's example:

$$3x^3 + 5y^3 + 7 = 0$$

Terminology:

- Quadratic curves satisfy the Local-to-Global principle
- Curves in general do not.

Question: Can we identify obstructions to C having rational points if $C(\mathbb{Q}_p) \neq \emptyset$ for all p ?

The Chevalley-Weil Theorem

Theorem: Let $\pi : D \rightarrow C$ be an unramified Galois cover. Then there is a finite collection of twists $\pi_\delta : D_\delta \rightarrow C$ such that

$$\bigcup_{\delta} \pi_\delta(D_\delta(\mathbb{Q})) = C(\mathbb{Q})$$

The Chevalley-Weil Theorem

Theorem: Let $\pi : D \rightarrow C$ be an unramified Galois cover. Then there is a finite collection of twists $\pi_\delta : D_\delta \rightarrow C$ such that

$$\bigcup_{\delta} \pi_\delta(D_\delta(\mathbb{Q})) = C(\mathbb{Q})$$

Computability: The set of twists is explicit, at least in principle:

$$\delta \in H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}_{\overline{\mathbb{Q}}}(D/C); S)$$

The Chevalley-Weil Theorem

Theorem: Let $\pi : D \rightarrow C$ be an unramified Galois cover. Then there is a finite collection of twists $\pi_\delta : D_\delta \rightarrow C$ such that

$$\bigcup_{\delta} \pi_\delta(D_\delta(\mathbb{Q})) = C(\mathbb{Q})$$

Computability: The set of twists is explicit, at least in principle:

$$\delta \in H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}_{\overline{\mathbb{Q}}}(D/C); S)$$

Selmer set:

$$\mathrm{Sel}^{(\pi)}(C/\mathbb{Q}) = \{\delta : D_\delta(\mathbb{Q}_p) \neq \emptyset \text{ for all } p\}$$

Covering criterion: If $\mathrm{Sel}^{(\pi)}(C/\mathbb{Q}) = \emptyset$ then $C(\mathbb{Q}) = \emptyset$.

Hyperelliptic curves

- $C : y^2 = f(x) = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0$ with n even

Hyperelliptic curves

- $C : y^2 = f(x) = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0$ with n even
- $A_k = k[\theta] = k[x]/(f(x))$
- $M_k = A_k^*/k^* A_k^{*2}$
- $\mu_k : \begin{array}{l} C(k) \rightarrow M \\ (x, y) \mapsto x - \theta \end{array}$

Hyperelliptic curves

- $C : y^2 = f(x) = f_n x^n + f_{n-1} x^{n-1} + \dots + f_0$ with n even
- $A_k = k[\theta] = k[x]/(f(x))$
- $M_k = A_k^*/k^* A_k^{*2}$
- $\mu_k : \begin{array}{ccc} C(k) & \rightarrow & M \\ (x, y) & \mapsto & x - \theta \end{array}$

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\mu} & M_{\mathbb{Q}} \\ \downarrow & & \downarrow r_p \\ C(\mathbb{Q}_p) & \xrightarrow{\mu_p} & M_{\mathbb{Q}_p} \end{array}$$

Definition:

$$\text{Sel}_{\text{fake}}^{(2)}(C/\mathbb{Q}) = \{\delta \in M_{\mathbb{Q}} : r_p(\delta) \in \mu_p(C(\mathbb{Q}_p)) \text{ for all } p\}$$

Hyperelliptic curves

- $C : y^2 = f(x) = f_n x^n + f_{n-1} x^{n-1} + \dots + f_0$ with n even
- $A_k = k[\theta] = k[x]/(f(x))$
- $M_k = A_k^*/k^* A_k^{*2}$
- $\mu_k : \begin{array}{ccc} C(k) & \rightarrow & M \\ (x, y) & \mapsto & x - \theta \end{array}$

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\mu} & M_{\mathbb{Q}} \\ \downarrow & & \downarrow r_p \\ C(\mathbb{Q}_p) & \xrightarrow{\mu_p} & M_{\mathbb{Q}_p} \end{array}$$

Definition:

$$\text{Sel}_{\text{fake}}^{(2)}(C/\mathbb{Q}) = \{\delta \in M_{\mathbb{Q}} : r_p(\delta) \in \mu_p(C(\mathbb{Q}_p)) \text{ for all } p\}$$

Theorem (B., Stoll):

$$\text{Sel}_{\text{fake}}^{(2)}(C/\mathbb{Q}) = \emptyset \text{ if and only if } \text{Sel}^{(2)}(C/\mathbb{Q}) = \emptyset$$

Question: How often are these methods successful in showing that $C(\mathbb{Q}) = \emptyset$?

$$V_n(B) = \{y^2 = f_n x^n + \cdots + f_0 : f_i \in \{-B, \dots, B\}\}$$

Hilbert's Tenth Problem

First approaches

Local-to-Global principle

The Chevalley-Weil
Theorem

Hyperelliptic curves

Asymptotics

An experiment

Other application

A new criterion

Question: How often are these methods successful in showing that $C(\mathbb{Q}) = \emptyset$?

$$V_n(B) = \{y^2 = f_n x^n + \cdots + f_0 : f_i \in \{-B, \dots, B\}\}$$

$$L_n(B) = \frac{\#\{C \in V_n(B) : C(\mathbb{Q}_p) = \emptyset \text{ for some } p\}}{\#V_n(B)}$$

$$S_n(B) = \frac{\#\{C \in V_n(B) : \text{Sel}^{(2)}(C/\mathbb{Q}) = \emptyset\}}{\#V_n(B)}$$

Hilbert's Tenth Problem

First approaches

Local-to-Global principle

The Chevalley-Weil
Theorem

Hyperelliptic curves

Asymptotics

An experiment

Other application

A new criterion

Question: How often are these methods successful in showing that $C(\mathbb{Q}) = \emptyset$?

$$V_n(B) = \{y^2 = f_n x^n + \cdots + f_0 : f_i \in \{-B, \dots, B\}\}$$

$$L_n(B) = \frac{\#\{C \in V_n(B) : C(\mathbb{Q}_p) = \emptyset \text{ for some } p\}}{\#V_n(B)}$$

$$S_n(B) = \frac{\#\{C \in V_n(B) : \text{Sel}^{(2)}(C/\mathbb{Q}) = \emptyset\}}{\#V_n(B)}$$

Theorem (Poonen, Stoll): $\lim_{B \rightarrow \infty} L_6(B) \approx 0.15$

Open problem $\lim_{B \rightarrow \infty} S_6(B) = ?$

Hilbert's Tenth Problem

First approaches

Local-to-Global principle

The Chevalley-Weil

Theorem

Hyperelliptic curves

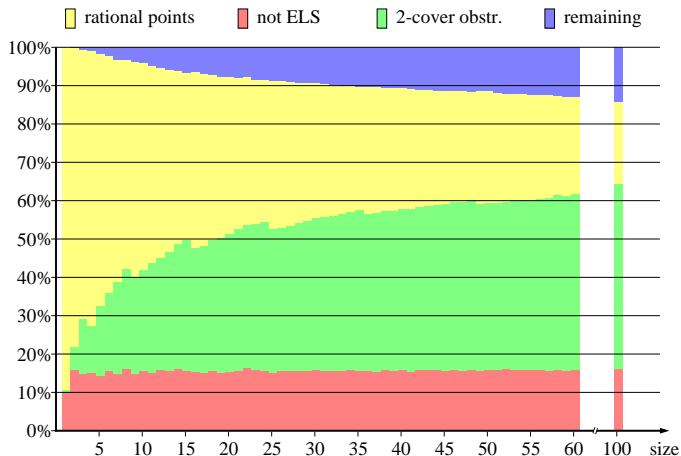
Asymptotics

An experiment

Other application

A new criterion

An experiment



Hilbert's Tenth Problem

First approaches

Local-to-Global principle

The Chevalley-Weil
Theorem

Hyperelliptic curves

Asymptotics

An experiment

Other application

A new criterion

Other application

Definition: A number $n \in \mathbb{Z}$ is called *congruent* if it occurs as the area of a right triangle with rational sides.

Other application

Definition: A number $n \in \mathbb{Z}$ is called *congruent* if it occurs as the area of a right triangle with rational sides.

Theorem (various): Let p be a prime

- If $p \equiv 5, 7 \pmod{8}$ then p is congruent
- If $p \equiv 3 \pmod{8}$ then p is not congruent
- If $p \equiv 1 \pmod{8}$ and $1 + i \not\equiv a^2 \pmod{p}$ for any a then p is not congruent

Other application

Definition: A number $n \in \mathbb{Z}$ is called *congruent* if it occurs as the area of a right triangle with rational sides.

Theorem (various): Let p be a prime

- If $p \equiv 5, 7 \pmod{8}$ then p is congruent
- If $p \equiv 3 \pmod{8}$ then p is not congruent
- If $p \equiv 1 \pmod{8}$ and $1 + i \not\equiv a^2 \pmod{p}$ for any a then p is not congruent

Proposition' (Hemenway): If a prime $p \equiv 1 \pmod{8}$ is congruent then

$$C_p : y^2 = p(x^4 - 4x^3 - 6x^2 - 12x - 7)$$

has a rational point.

Definition: A number $n \in \mathbb{Z}$ is called *congruent* if it occurs as the area of a right triangle with rational sides.

Theorem (various): Let p be a prime

- If $p \equiv 5, 7 \pmod{8}$ then p is congruent
- If $p \equiv 3 \pmod{8}$ then p is not congruent
- If $p \equiv 1 \pmod{8}$ and $1 + i \not\equiv a^2 \pmod{p}$ for any a then p is not congruent

Proposition' (Hemenway): If a prime $p \equiv 1 \pmod{8}$ is congruent then

$$C_p : y^2 = p(x^4 - 4x^3 - 6x^2 - 12x - 7)$$

has a rational point.

Remark: If $1 + i \equiv a^2 \pmod{p}$ then C_p has no local obstruction to having rational points.

A new criterion for congruent primes

Theorem: Let $p \equiv 1 \pmod{8}$ with $1 + i \equiv a^2 \pmod{p}$.

Let

$$L = \mathbb{Q}(\sqrt{1+i}, \sqrt{2})$$

and factorize p in L as:

$$p = \pi_1 \pi_2 \pi_3 \cdots \pi_8 \text{ (labelling is important here)}$$

If

$$\left(\frac{\pi_2 \pi_4 \pi_6 \pi_8 \sqrt{1+i}}{\pi_1} \right) = -1$$

then

$$\text{Sel}^{(2)}(C_p/\mathbb{Q}) = \emptyset$$

Application: $p = 10^{100} + 20601$ is not congruent.