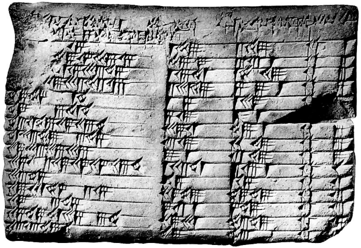
Diophantine equations, local-global principles and arithmetic statistics

Rachel Newton
King's College London

October 2022

Diophantine equations



Mathematicians working on Diophantine equations study the integer solutions to polynomial equations with integer coefficients.

E.g. the Pythagorean equation $a^2 + b^2 = c^2$ has the integer solution $a = 3, b = 4, c = 5$.

Hilbert's 10th problem

Problem 10 (Hilbert, 1900)

Construct an algorithm which can decide whether any given Diophantine equation has a solution.

Hilbert's 10th problem

Theorem (Matiyasevich, Robinson, Davis, Putnam, 1970)

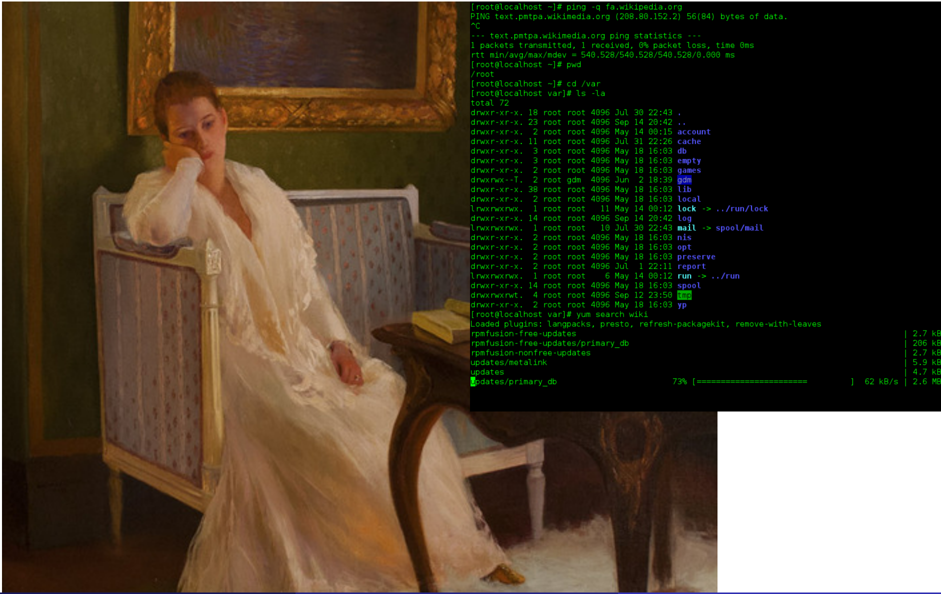
No such algorithm exists.

Question

Hilbert's 10th problem over $\mathbb{Q}$?

Wide open.

Searching for rational points



Proving no rational points exist

Let $X/\mathbb{Q}$ be an algebraic variety.

$$X(\mathbb{Q}) \subset X(\mathbb{R})$$

so

$$X(\mathbb{R}) = \emptyset \Longrightarrow X(\mathbb{Q}) = \emptyset.$$

$X(\mathbb{R})$ is easier to deal with than $X(\mathbb{Q})$ because $\mathbb{R}$ is complete.

The real world is not enough

But

$$X(\mathbb{R}) \neq \emptyset \not\Longrightarrow X(\mathbb{Q}) \neq \emptyset.$$

E.g. $x^2 = 2$ has real solutions but no rational solutions.

$\mathbb{R}$ is not the only completion of $\mathbb{Q}$.

The other completions are $\mathbb{Q}_p$, for p prime.

$$X(\mathbb{Q}) \subset X(\mathbb{Q}_p)$$

so

$$X(\mathbb{Q}_p) = \emptyset \Longrightarrow X(\mathbb{Q}) = \emptyset.$$

Idea: use all the completions of $\mathbb{Q}$ at once.

The Hasse principle

Let $X/\mathbb{Q}$ be a nice variety.

$$X(\mathbb{Q}) \subset X(\mathbb{R}) \times \prod_p X(\mathbb{Q}_p) =: X(\mathbb{A}_\mathbb{Q}) \quad \text{adelic points}$$

$$Q \mapsto (Q, Q, Q, Q, Q, \dots)$$

$$X(\mathbb{Q}) \neq \emptyset \Longrightarrow X(\mathbb{A}_\mathbb{Q}) \neq \emptyset$$

Definition

If " $\Longleftarrow$ " holds, we say the **Hasse principle** holds.

What causes failures of the Hasse principle?

Brauer–Manin obstructions

Manin, 1970: Let $\mathrm{Br}\, X = \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m)$. There's a pairing

$$X(\mathbb{A}_\mathbb{Q}) \times \mathrm{Br}\, X \quad \to \quad \mathbb{Q}/\mathbb{Z}$$

such that $\overline{X(\mathbb{Q})} \subset X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} :=$ adelic points orthogonal to $\mathrm{Br}\, X$.

- Suppose $X(\mathbb{A}_\mathbb{Q}) \neq \emptyset$ but $X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} = \emptyset$. Then $X(\mathbb{Q}) = \emptyset$.
  Brauer–Manin obstruction to the Hasse principle

Weak approximation

Weak approximation holds if $X(\mathbb{Q})$ is dense in $X(\mathbb{A}_{\mathbb{Q}})$.

We have

$$\overline{X(\mathbb{Q})} \subset X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} \subset X(\mathbb{A}_{\mathbb{Q}}).$$

- If $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} \neq X(\mathbb{A}_{\mathbb{Q}})$ then $\overline{X(\mathbb{Q})} \neq X(\mathbb{A}_{\mathbb{Q}})$.
  Brauer–Manin obstruction to weak approximation

The Brauer–Manin pairing

The Brauer–Manin pairing is given by

$$\begin{array}{rcl} X(\mathbb{A}_{\mathbb{Q}}) \times \operatorname{Br} X & \to & \mathbb{Q}/\mathbb{Z} \\ ((Q_p)_p \ , \ \mathcal{A}) & \mapsto & \displaystyle\sum_{p \leq \infty} \mathcal{A}(Q_p) \end{array}$$

Let $X(\mathbb{A}_{\mathbb{Q}})^{\mathcal{A}}$ denote the set of adelic points orthogonal to $\mathcal{A} \in \operatorname{Br} X$.

Lemma

If $|\mathcal{A}| : X(\mathbb{Q}_v) \to \mathbb{Q}/\mathbb{Z}, Q_v \mapsto \mathcal{A}(Q_v)$, *is non-constant for some* v *then* $X(\mathbb{A}_{\mathbb{Q}})^{\mathcal{A}} \neq X(\mathbb{A}_{\mathbb{Q}})$, *i.e.* $\mathcal{A}$ **obstructs weak approximation.**

Proof.

Let $(P_w)_w \in X(\mathbb{A}_{\mathbb{Q}})$. If $\sum_w \mathcal{A}(P_w) = 0$ then replace P_v with some Q_v such that $\mathcal{A}(Q_v) \neq \mathcal{A}(P_v)$. □

The Brauer group

The Brauer group has two parts:

- $\operatorname{Br}_1 X = \ker(\operatorname{Br} X \to \operatorname{Br} \overline{X})$ "algebraic part" – easy to calculate
- $\operatorname{Br} X / \operatorname{Br}_1 X$ "transcendental part" – difficult to calculate, mostly unknown

Transcendental Brauer group calculations

- Conic bundles over $\mathbb{P}^2$ (Artin–Mumford, 1972)
- Diagonal quartic surfaces $ax^4 + by^4 + cz^4 + dw^4 = 0$ over $\mathbb{Q}$ (Ieronymou–Skorobogatov, 2014)
- Products $E \times E$ of CM elliptic curves (N., 2016)
- Non-diagonal quartic surfaces $ax^4 + bxy^3 + czw^3 + dz^4 = 0$ over $\mathbb{Q}$ (Alaa Tawfik–N., work in progress)

Example of a transcendental Brauer–Manin obstruction

Theorem (Alaa Tawfik–N., to appear)

Let $X/\mathbb{Q}$ be a Kummer surface with affine equation

$$w^2 = (x^3 + c)(t^3 + d).$$

$\operatorname{Br} X$ *contains a transcendental element of order* $5 \iff 80cd \in \mathbb{Q}(\zeta_3)^{\times 6}$.

Moreover, such an element always obstructs weak approximation.

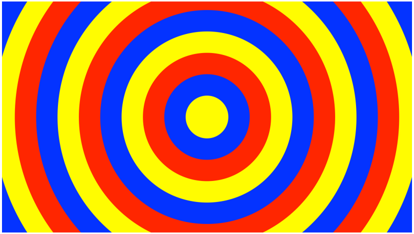
Uses work of Ieronymou–Skorobogatov where they obtain similar results for diagonal quartic surfaces.

How do the evaluation maps vary on p-adic discs?

Let $Q_p \in X(\mathbb{Q}_p)$.

- If $\mathcal{A}$ has order coprime to p then $\mathcal{A}(Q_p)$ only depends on Q_p mod p.
- If $\mathcal{A}$ has order p^n then $\mathcal{A}(Q_p)$ could depend on Q_p mod p^2 or mod p^3 etc.

Wild evaluation maps



Bright–N., 2020

For $\mathcal{A} \in \operatorname{Br} X$ of order p^n, we:

- calculate m such that $\mathcal{A}(Q_p)$ only depends on Q_p mod p^m
- show that $\mathcal{A}(Q_p)$ varies linearly on discs of points that are the same mod p^{m-1}
- if $p \mid m$, can get quadratic variation on larger discs

Which primes can be involved in the Brauer–Manin obstruction?

Let $\mathcal{A} \in \operatorname{Br} X$.

Question (Swinnerton-Dyer, 2010)

Suppose that $\operatorname{Pic} \bar{X}$ is torsion-free. Let p be a prime of good reduction for X (i.e. X mod p is smooth). Is $\mathcal{A}(Q_p)$ constant as Q_p varies in $X(\mathbb{Q}_p)$?

Equivalently, let $S = \{\text{primes of bad reduction}\} \cup \{\infty\}$. Does

$$X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = Z \times \prod_{p \notin S} X(\mathbb{Q}_p),$$

where $Z \subset \prod_{p \in S} X(\mathbb{Q}_p)$?

Does the Brauer–Manin obstruction involve only primes of bad reduction and infinite primes?

Which primes can be involved in the Brauer–Manin obstruction?

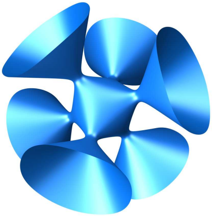
Theorem (Bright–N., 2020)

If $\mathrm{H}^0(X, \Omega^2_X) \neq 0$ *then every prime of good ordinary reduction is involved in a Brauer–Manin obstruction over some finite extension of the base field.*

Consequence:

The answer to Swinnerton-Dyer's question is no in general for K3 surfaces over number fields.

Image by Alessandra Sarti.



$1 + x^4 + y^4 + z^4 + a(x^2 + y^2 + z^2 + 1)^2 = 0, \ a = -0.49$

Which primes can be involved in the Brauer–Manin obstruction?

Question

Suppose $\operatorname{Pic} \bar{X}$ is torsion-free. Is there a finite set S of primes that can be involved in the Brauer–Manin obstruction for X? Can we describe S?

Which primes can be involved in the Brauer–Manin obstruction?

Theorem (Bright–N., 2020)

Suppose $\operatorname{Pic} \bar{X}$ *is torsion-free. Then the finite set* S *consists of:*

- *primes of bad reduction;*
- *infinite primes;*
- *even primes;*
- *ramified primes;*
- *primes for which* $\mathrm{H}^0(X \bmod p, \Omega^1) \neq 0$ *(not needed if* X *is a K3 surface).*

E.g. for a K3 surface over $\mathbb{Q}$, the relevant primes are

$$\{\text{primes of bad reduction}\} \cup \{2, \infty\}.$$

How often does the Hasse principle fail?

How often does the Hasse principle fail?

Family	**Proportion of failures**
$y^2 + z^2 = (at^2 + b)(ct^2 + d)$ (de la Bretèche–Browning, 2013)	0%
Hyperelliptic curves $z^2 = a_0 x^{2g+2} + a_1 x^{2g+1} y + \cdots + a_{2g+2} y^{2g+2}$ (Bhargava, 2013)	$> 0\%$ for $g = 1$, $> 50\%$ for $g \geq 2$, $> 99\%$ for $g \geq 10$
Plane cubics (Bhargava, 2014)	$> 0\%$ conjecturally $1 - 1/3$

Norm one tori

Let $L = \mathbb{Q}(\omega)$, degree d extension. The norm one torus for $L/\mathbb{Q}$ is the affine variety

$$T_{L/\mathbb{Q}} : N_{L/\mathbb{Q}}(x_0 + x_1\omega + \cdots + x_{d-1}\omega^{d-1}) = 1.$$

Its torsors are the affine varieties

$$T_{L/\mathbb{Q},\alpha} : \; N_{L/\mathbb{Q}}(x_0 + x_1\omega + \cdots + x_{d-1}\omega^{d-1}) = \alpha.$$

for $\alpha \in \mathbb{Q}^\times$.

Local and global points

$$T_{L/\mathbb{Q},\alpha}: \ N_{L/\mathbb{Q}}(x_0 + x_1\omega + \cdots + x_{d-1}\omega^{d-1}) = \alpha$$

$T_{L/\mathbb{Q},\alpha}(\mathbb{Q}) \neq \emptyset \iff \alpha$ is in the image of $N_{L/\mathbb{Q}} : L \to \mathbb{Q}$.

$T_{L/\mathbb{Q},\alpha}(\mathbb{Q}_p) \neq \emptyset \iff \alpha$ is in the image of $N_{L/\mathbb{Q}} : L \otimes \mathbb{Q}_p \to \mathbb{Q}_p$.

$T_{L/\mathbb{Q},\alpha}(\mathbb{R}) \neq \emptyset \iff \alpha$ is in the image of $N_{L/\mathbb{Q}} : L \otimes \mathbb{R} \to \mathbb{R}$.

Local and global points

Example

$L = \mathbb{Q}(i), \alpha = -2.$

$$N_{L/\mathbb{Q}}(x + yi) = (x + yi)(x - yi) = x^2 + y^2 = -2$$

$L \otimes \mathbb{R} = \mathbb{R}(i) = \mathbb{C}$. Image of $N_{L/\mathbb{Q}} : \mathbb{C}^\times \to \mathbb{R}^\times$ is $\mathbb{R}_{>0}$.

No real solution $\implies$ no rational (or "global") solution.

Local and global points

If $\alpha \neq 0$ is in the image of $N_{L/\mathbb{Q}} : L \to \mathbb{Q}$, say

"α is a global norm from $L/\mathbb{Q}$".

If $\alpha \neq 0$ is in the image of $N_{L/\mathbb{Q}} : L \otimes \mathbb{R} \to \mathbb{R}$ and in the image of $N_{L/\mathbb{Q}} : L \otimes \mathbb{Q}_p \to \mathbb{Q}_p$ for all p, say

"α is an everywhere local norm from $L/\mathbb{Q}$".

$$\{\text{global norms from } L/\mathbb{Q}\} \subset \{\text{everywhere local norms from } L/\mathbb{Q}\}.$$

The Hasse norm principle

$$Ш(T_{L/\mathbb{Q}}) = \frac{\{\text{everywhere local norms from } L/\mathbb{Q}\}}{\{\text{global norms from } L/\mathbb{Q}\}}$$

- If $Ш(T_{L/\mathbb{Q}}) = 1$ then the Hasse principle holds for all $T_{L/\mathbb{Q},\alpha}$ and we say the Hasse norm principle holds for $L/\mathbb{Q}$.
- If $Ш(T_{L/\mathbb{Q}}) \neq 1$ then there are rational numbers α which are everywhere locally norms from $L/\mathbb{Q}$ but not global norms. The Hasse principle fails for these $T_{L/\mathbb{Q},\alpha}$.

How often does the Hasse principle fail?

Family	Proportion of failures
$y^2 + z^2 = (at^2 + b)(ct^2 + d)$ (de la Bretèche–Browning, 2013)	0%
Hyperelliptic curves $z^2 = a_0 x^{2g+2} + a_1 x^{2g+1} y + \cdots + a_{2g+2} y^{2g+2}$ (Bhargava, 2013)	$> 0\%$ for $g = 1$, $> 50\%$ for $g \geq 2$, $> 99\%$ for $g \geq 10$
Plane cubics (Bhargava, 2014)	$> 0\%$ conjecturally $1 - 1/3$
Torsors for a norm one torus $T/\mathbb{Q}$ (Browning–N., 2016)	$1 - 1/\lvert Ш(T)\rvert$

Statistics of the Hasse norm principle

Let G be a finite abelian group.

A G-extension is a Galois extension with Galois group G.

Theorem (Frei–Loughran–N., 2018)

When ordered by conductor, 100% of G-extensions satisfy the Hasse norm principle.

We used this to give an asymptotic formula for the number of G-extensions from which a given element α is a norm.

S_4-quartics with prescribed norms

- Let $\alpha \in \mathbb{Q}^\times$.
- Write $N(B)$ for the number of S_4-quartic extensions $L/\mathbb{Q}$ with discriminant at most B.
- Write $N(B;\alpha)$ for the number of such extensions with $\alpha \in N_{L/\mathbb{Q}}(L^\times)$.

Theorem (Monnet, 2022)

$$0 < \lim_{B\to\infty} \frac{N(B;\alpha)}{N(B)} \leq 1,$$

with equality if and only if $\alpha \in \mathbb{Q}^{\times 4}$.

Statistics of the Hasse norm principle for non-abelian extensions

Theorem (N.–Varma, in preparation)

The Hasse norm principle holds for 100% of S_4-octics.

$$\mathcal{F}_{12} = \{\text{Degree } 12\ S_4\text{-fields fixed by a double transposition}\}.$$

The behaviour in this family is strikingly different from that of S_4-octics.

Theorem (N.–Varma, in preparation)

The Hasse norm principle fails for a positive proportion of fields in $\mathcal{F}_{12}$.

Thank you for your attention.