Diophantine equations
and when to quit trying to solve them

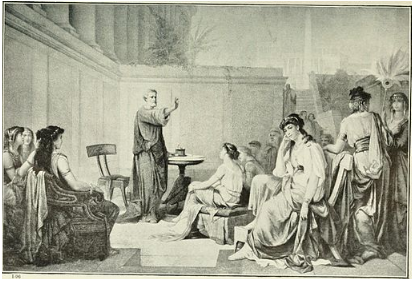
Rachel Newton

King's College London

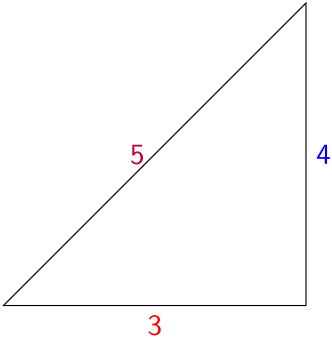
April 2023

Diophantine equations

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

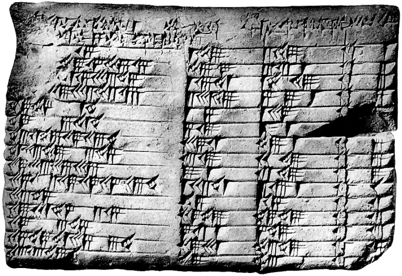


E.g. the Pythagorean equation $a^2 + b^2 = c^2$ has the integer solution $a = 3, b = 4, c = 5$.



$$3^2 + 4^2 = 5^2$$

Plimpton 322 (c. 1800 BC)



$$
\begin{aligned}
119^2 + 120^2 &= 169^2 \\
3367^2 + 3456^2 &= 4825^2 \\
4601^2 + 4800^2 &= 6649^2 \\
12709^2 + 13500^2 &= 18541^2
\end{aligned}
$$

Rational points on algebraic varieties

Let $f(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$.

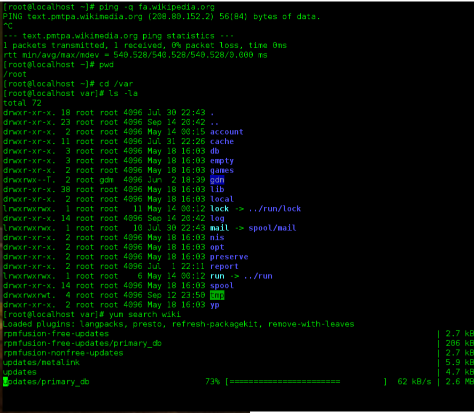
Let $X/\mathbb{Q}$ be the variety defined by $f(x_1, \ldots, x_n) = 0$.

The set of **rational points** on X is

$$X(\mathbb{Q}) = \{(x_1, \ldots, x_n) \in \mathbb{Q}^n \mid f(x_1, \ldots, x_n) = 0\}.$$

E.g. $(0, 1)$ is a rational point on the unit circle $x^2 + y^2 - 1 = 0$.

Searching for rational points



Using $\mathbb{R}$ to prove that no rational points exist

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

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

so

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

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

The real world is not enough

But

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

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

The real world is not enough

But

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

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

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

The real world is not enough

But

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

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

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

$$\mathbb{R} = \frac{\{\text{Cauchy sequences in } \mathbb{Q} \text{ with respect to } |\cdot|\}}{\{\text{sequences in } \mathbb{Q} \text{ converging to } 0 \text{ with respect to } |\cdot|\}}$$

i.e. $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|$.

The real world is not enough

But

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

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

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

$$\mathbb{R} = \frac{\{\text{Cauchy sequences in } \mathbb{Q} \text{ with respect to } |\cdot|\}}{\{\text{sequences in } \mathbb{Q} \text{ converging to } 0 \text{ with respect to } |\cdot|\}}$$

i.e. $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|$.

E.g. π can be represented by the Cauchy sequence

$$3, 3.1, 3.14, 3.141, 3.1415, 3.14159, \ldots$$

or by

$$3 + 1, 3.1 + 1/2, 3.14 + 1/3, 3.141 + 1/4, 3.1415 + 1/5, 3.14159 + 1/6, \ldots$$

Entering the p-adic world

Let p be a prime. Define the p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$ by

$$\left|p^r \frac{a}{b}\right|_p = p^{-r}$$

where $r, a, b \in \mathbb{Z}$ and $p \nmid a, b$. We also set $|0|_p = 0$.

Entering the p-adic world

Let p be a prime. Define the p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$ by

$$\left|p^r \frac{a}{b}\right|_p = p^{-r}$$

where $r, a, b \in \mathbb{Z}$ and $p \nmid a, b$. We also set $|0|_p = 0$.

E.g. $5, 5^2, 5^3, 5^4, \dots \to 0$ with respect to $|\cdot|_5$.

Entering the p-adic world

Let p be a prime. Define the p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$ by

$$\left|p^r \frac{a}{b}\right|_p = p^{-r}$$

where $r, a, b \in \mathbb{Z}$ and $p \nmid a, b$. We also set $|0|_p = 0$.

E.g. $5, 5^2, 5^3, 5^4, \cdots \to 0$ with respect to $|\cdot|_5$.

$1, 11, 111, 1111, 11111, \cdots \to -1/9$ with respect to $|\cdot|_5$.

The p-adic numbers

$$\mathbb{Q}_p = \frac{\{\text{Cauchy sequences in } \mathbb{Q} \text{ with respect to } |\cdot|_p\}}{\{\text{sequences in } \mathbb{Q} \text{ converging to } 0 \text{ with respect to } |\cdot|_p\}}$$

i.e. $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

The p-adic numbers

$$\mathbb{Q}_p = \frac{\{\text{Cauchy sequences in } \mathbb{Q} \text{ with respect to } |\cdot|_p\}}{\{\text{sequences in } \mathbb{Q} \text{ converging to } 0 \text{ with respect to } |\cdot|_p\}}$$

i.e. $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Concretely, elements of $\mathbb{Q}_p$ look like

$$\sum_{n=N}^{\infty} a_n p^n, \qquad a_n \in \{0, 1, \ldots, p-1\}, \ N \in \mathbb{Z}.$$

The Hasse principle

$$X(\mathbb{Q}) \subset X(\mathbb{R}) \times \prod_p X(\mathbb{Q}_p) = X(\mathbb{A}_\mathbb{Q})$$

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

The Hasse principle

$$X(\mathbb{Q}) \subset X(\mathbb{R}) \times \prod_p X(\mathbb{Q}_p) = X(\mathbb{A}_\mathbb{Q})$$

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

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

The Hasse principle

$$X(\mathbb{Q}) \subset X(\mathbb{R}) \times \prod_p X(\mathbb{Q}_p) = X(\mathbb{A}_{\mathbb{Q}})$$

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

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

Definition

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

The Hasse–Minkowski Theorem

Theorem (Hasse–Minkowski)

The Hasse principle holds for quadratic forms. I.e. a quadratic form over $\mathbb{Q}$ has a non-trivial zero over $\mathbb{Q}$ iff it has non-trivial zeros over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all primes p.

A counterexample to the Hasse principle

Example (Lind, Reichardt)

The curve

$$C : 2y^2 = x^4 - 17z^4$$

has points over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all p but no points over $\mathbb{Q}$.

A counterexample to the Hasse principle

Example (Lind, Reichardt)

The curve

$$C : 2y^2 = x^4 - 17z^4$$

has points over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all p but no points over $\mathbb{Q}$.

How do we prove that $C(\mathbb{Q}) = \emptyset$?

A counterexample to the Hasse principle

Example (Lind, Reichardt)

The curve

$$C : 2y^2 = x^4 - 17z^4$$

has points over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all p but no points over $\mathbb{Q}$.

How do we prove that $C(\mathbb{Q}) = \emptyset$?

We need a tool that combines information at different primes.

Hilbert symbols

Let $a, b \in \mathbb{Q}_p \setminus \{0\}$. Define the Hilbert symbol $(a, b)_p$ as follows:

$$(a, b)_p = \begin{cases} 1/2 & \text{if } as^2 + bt^2 = u^2 \text{ has no nontrivial solution over } \mathbb{Q}_p; \\ 0 & \text{otherwise.} \end{cases}$$

Hilbert symbols

Let $a, b \in \mathbb{Q}_p \setminus \{0\}$. Define the Hilbert symbol $(a, b)_p$ as follows:

$$(a,b)_p = \begin{cases} 1/2 & \text{if } as^2 + bt^2 = u^2 \text{ has no nontrivial solution over } \mathbb{Q}_p; \\ 0 & \text{otherwise.} \end{cases}$$

Similarly, for $a, b \in \mathbb{R} \setminus \{0\}$, write

$$(a,b)_\infty = \begin{cases} 1/2 & \text{if } as^2 + bt^2 = u^2 \text{ has no nontrivial solution over } \mathbb{R}; \\ 0 & \text{otherwise.} \end{cases}$$

Hilbert symbols

Theorem (equivalent to quadratic reciprocity)

Let $a, b \in \mathbb{Q} \setminus \{0\}$*. Then*

$$\sum_{p \leq \infty} (a, b)_p \in \mathbb{Z}.$$

Returning to Lind and Reichardt's counterexample

Recall the curve

$$C : 2y^2 = x^4 - 17z^4.$$

The symbol $(y, 17)$ can be evaluated at a $\mathbb{Q}_p$-point or an $\mathbb{R}$-point of C to give a Hilbert symbol.

Returning to Lind and Reichardt's counterexample

Recall the curve

$$C : 2y^2 = x^4 - 17z^4.$$

The symbol $(y, 17)$ can be evaluated at a $\mathbb{Q}_p$-point or an $\mathbb{R}$-point of C to give a Hilbert symbol.

E.g. let $Q = (\sqrt{2}, \sqrt{2}, 0) \in C(\mathbb{R})$. Then

$$(y, 17)(Q) = (y_Q, 17)_\infty = (\sqrt{2}, 17)_\infty.$$

Returning to Lind and Reichardt's counterexample

Recall the curve

$$C : 2y^2 = x^4 - 17z^4.$$

The symbol $(y, 17)$ can be evaluated at a $\mathbb{Q}_p$-point or an $\mathbb{R}$-point of C to give a Hilbert symbol.

E.g. let $Q = (\sqrt{2}, \sqrt{2}, 0) \in C(\mathbb{R})$. Then

$$(y, 17)(Q) = (y_Q, 17)_\infty = (\sqrt{2}, 17)_\infty.$$

Note that

$$\sqrt{2}s^2 + 17t^2 = u^2$$

has the solution $(0, 1, \sqrt{17})$ over $\mathbb{R}$. Therefore, $(\sqrt{2}, 17)_\infty = 0$.

Returning to Lind and Reichardt's counterexample

One can show that for any $Q \in C(\mathbb{Q})$, we have

$$(y_Q, 17)_\infty = 0 \text{ and } (y_Q, 17)_p = 0 \text{ for all } p \neq 17.$$

Returning to Lind and Reichardt's counterexample

One can show that for any $Q \in C(\mathbb{Q})$, we have

$$(y_Q, 17)_\infty = 0 \text{ and } (y_Q, 17)_p = 0 \text{ for all } p \neq 17.$$

E.g. $\sqrt{17} \in \mathbb{Q}_{13}$ so

$$y_Q s^2 + 17t^2 = u^2$$

has the solution $(0, 1, \sqrt{17})$ over $\mathbb{Q}_{13}$. Hence, $(y_Q, 17)_{13} = 0$.

Returning to Lind and Reichardt's counterexample

One can show that for any $Q \in C(\mathbb{Q})$, we have

$$(y_Q, 17)_\infty = 0 \text{ and } (y_Q, 17)_p = 0 \text{ for all } p \neq 17.$$

E.g. $\sqrt{17} \in \mathbb{Q}_{13}$ so

$$y_Q s^2 + 17t^2 = u^2$$

has the solution $(0, 1, \sqrt{17})$ over $\mathbb{Q}_{13}$. Hence, $(y_Q, 17)_{13} = 0$.

On the other hand, we will show that $(y_Q, 17)_{17} = 1/2$. This gives

$$\sum_{p \leq \infty} (y_Q, 17)_p = 1/2 \notin \mathbb{Z},$$

contradicting the reciprocity theorem. This implies that $C(\mathbb{Q}) = \emptyset$.

Proving that $(y_Q, 17)_{17} = 1/2$

Let $Q = (x_Q, y_Q, z_Q) \in C(\mathbb{Q})$. So

$$2y_Q^2 = x_Q^4 - 17z_Q^4. \qquad (1)$$

Rescaling, we can assume that $x_Q, y_Q, z_Q \in \mathbb{Z}$.

Proving that $(y_Q, 17)_{17} = 1/2$

Let $Q = (x_Q, y_Q, z_Q) \in C(\mathbb{Q})$. So

$$2y_Q^2 = x_Q^4 - 17z_Q^4. \tag{1}$$

Rescaling, we can assume that $x_Q, y_Q, z_Q \in \mathbb{Z}$.

Suppose for contradiction that

$$y_Q s^2 + 17t^2 = u^2$$

has a nontrivial solution over $\mathbb{Q}_{17}$. Then $y_Q \equiv (u/s)^2 \pmod{17}$.

Proving that $(y_Q, 17)_{17} = 1/2$

Let $Q = (x_Q, y_Q, z_Q) \in C(\mathbb{Q})$. So

$$2y_Q^2 = x_Q^4 - 17z_Q^4. \tag{1}$$

Rescaling, we can assume that $x_Q, y_Q, z_Q \in \mathbb{Z}$.

Suppose for contradiction that

$$y_Q s^2 + 17t^2 = u^2$$

has a nontrivial solution over $\mathbb{Q}_{17}$. Then $y_Q \equiv (u/s)^2 \pmod{17}$. Plugging this into (1) modulo 17 gives

$$2(u/s)^4 \equiv x_Q^4 \pmod{17}.$$

Proving that $(y_Q, 17)_{17} = 1/2$

Let $Q = (x_Q, y_Q, z_Q) \in C(\mathbb{Q})$. So

$$2y_Q^2 = x_Q^4 - 17z_Q^4. \tag{1}$$

Rescaling, we can assume that $x_Q, y_Q, z_Q \in \mathbb{Z}$.

Suppose for contradiction that

$$y_Q s^2 + 17t^2 = u^2$$

has a nontrivial solution over $\mathbb{Q}_{17}$. Then $y_Q \equiv (u/s)^2 \pmod{17}$.
Plugging this into (1) modulo 17 gives

$$2(u/s)^4 \equiv x_Q^4 \pmod{17}.$$

Hence 2 is a 4th power modulo 17. This is a contradiction because the only 4th powers modulo 17 are $0, \pm 1, \pm 4$. So $(y_Q, 17)_{17} = 1/2$. □

The Brauer group

The symbol $(y, 17)$ is an element in the Brauer group of C, written $\mathrm{Br}\, C$. The 2-torsion part of the Brauer group is made up of elements like this.

The Brauer group

The symbol $(y, 17)$ is an element in the Brauer group of C, written $\mathrm{Br}\, C$. The 2-torsion part of the Brauer group is made up of elements like this.

Let X be a nice variety and let $\mathcal{A} \in \mathrm{Br}\, X$. For all $p \leq \infty$, we have evaluation maps

$$X(\mathbb{Q}_p) \times \mathrm{Br}\, X \to \mathbb{Q}/\mathbb{Z}$$
$$(Q_p, \mathcal{A}) \mapsto \mathcal{A}(Q_p).$$

The Brauer group

The symbol $(y, 17)$ is an element in the Brauer group of C, written $\mathrm{Br}\, C$. The 2-torsion part of the Brauer group is made up of elements like this.

Let X be a nice variety and let $\mathcal{A} \in \mathrm{Br}\, X$. For all $p \leq \infty$, we have evaluation maps

$$\begin{aligned} X(\mathbb{Q}_p) \times \mathrm{Br}\, X &\to \mathbb{Q}/\mathbb{Z} \\ (Q_p, \mathcal{A}) &\mapsto \mathcal{A}(Q_p). \end{aligned}$$

Recalling that $X(\mathbb{A}_\mathbb{Q}) = \prod_{p \leq \infty} X(\mathbb{Q}_p)$, we obtain a pairing

$$\begin{aligned} X(\mathbb{A}_\mathbb{Q}) \times \mathrm{Br}\, X &\to \mathbb{Q}/\mathbb{Z} \\ ((Q_p)_{p \leq \infty}, \mathcal{A}) &\mapsto \sum_{p \leq \infty} \mathcal{A}(Q_p). \end{aligned}$$

Key observation (Manin, 1970):

$$X(\mathbb{Q}) \subset \left\{ (Q_p)_{p\leq\infty} \in X(\mathbb{A}_{\mathbb{Q}}) \mid \forall \mathcal{A} \in \operatorname{Br} X,\ \sum_{p\leq\infty} \mathcal{A}(Q_p) = 0 \in \mathbb{Q}/\mathbb{Z} \right\}.$$

The set on the right-hand side is the Brauer–Manin set, denoted $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$.

Brauer–Manin obstructions

Key observation (Manin, 1970):

$$X(\mathbb{Q}) \subset \left\{ (Q_p)_{p\leq\infty} \in X(\mathbb{A}_\mathbb{Q}) \mid \forall \mathcal{A} \in \operatorname{Br} X, \sum_{p\leq\infty} \mathcal{A}(Q_p) = 0 \in \mathbb{Q}/\mathbb{Z} \right\}.$$

The set on the right-hand side is the Brauer–Manin set, denoted $X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}}$.

- Suppose $X(\mathbb{A}_\mathbb{Q}) \neq \emptyset$ but $X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} = \emptyset$. Then $X(\mathbb{Q}) = \emptyset$.

Brauer–Manin obstructions

Key observation (Manin, 1970):

$$X(\mathbb{Q}) \subset \Big\{(Q_p)_{p\leq\infty} \in X(\mathbb{A}_\mathbb{Q}) \mid \forall \mathcal{A} \in \operatorname{Br} X,\ \sum_{p\leq\infty} \mathcal{A}(Q_p) = 0 \in \mathbb{Q}/\mathbb{Z}\Big\}.$$

The set on the right-hand side is the Brauer–Manin set, denoted $X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}}$.

- 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

Computing the Brauer–Manin set

To compute $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$, for each $\mathcal{A} \in \mathrm{Br}\, X$ we need to understand how $\mathcal{A}(Q_p)$ varies as Q_p varies in $X(\mathbb{Q}_p)$.

Computing the Brauer–Manin set

To compute $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$, for each $\mathcal{A} \in \mathrm{Br}\, X$ we need to understand how $\mathcal{A}(Q_p)$ varies as Q_p varies in $X(\mathbb{Q}_p)$.

For example, if $\mathcal{A}$ has order n then $\mathcal{A}(Q_p) \in \frac{1}{n}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$.

Computing the Brauer–Manin set

To compute $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$, for each $\mathcal{A} \in \operatorname{Br} X$ we need to understand how $\mathcal{A}(Q_p)$ varies as Q_p varies in $X(\mathbb{Q}_p)$.

For example, if $\mathcal{A}$ has order n then $\mathcal{A}(Q_p) \in \frac{1}{n}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$.

If for some p all values in $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ are attained then $X(\mathbb{A}_{\mathbb{Q}})^{\mathcal{A}} \neq \emptyset$, i.e. $\mathcal{A}$ **does not obstruct the Hasse principle**.

Computing the Brauer–Manin set

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

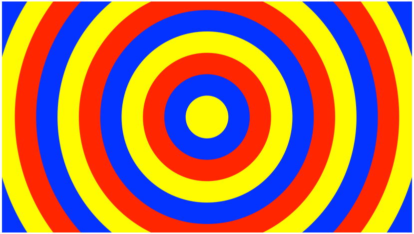
- If $\mathcal{A}$ has order coprime to p then $\mathcal{A}(Q_p)$ only depends on Q_p mod p.

Computing the Brauer–Manin set

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

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

Wild evaluation maps



Bright–N., 2020

For $\mathcal{A} \in \operatorname{Br} X$ of order p, 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}...
- ...unless $p \mid m$, when variation can be quadratic

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

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

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

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

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

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

Theorem (Bright–N., 2020)

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

Theorem (Margherita Pagano, 2021)

Let

$$X : x^3y + y^3z + z^3w + w^3x + xyzw = 0$$

and let $\mathcal{A} = \left(\frac{z^3+w^2x+xyz}{x^3}, \frac{-z}{x}\right) \in \mathrm{Br}\, X$. *Then 2 is a prime of good reduction for* X *and* $\mathcal{A}(Q_2)$ *is not constant as* Q_2 *varies in* $X(\mathbb{Q}_2)$.

Career overview

2021 – present Reader in Number Theory at KCL

2016 – 2021 Lecturer then Assoc. Prof. at Reading

2012 – 2015 Postdoc at Leiden, MPIM Bonn, IHÉS

2008 – 2012 PhD Cambridge

2007 – 2008 Part III Cambridge

2004 – 2007 BSc Warwick

Some things I learnt during my career

- Research is the primary criterion

  (for academic teaching and research jobs)
- Be strategic re teaching experience
  - Check out the Nesin Maths Village!
- Give good, comprehensible talks and lots of them. Ask for honest feedback.
  - Any talk in Germany is potentially a job talk (this may also apply elsewhere)
- Talk to big shots at conferences

Some more things I learnt during my career

- The sniper versus the scattergun approach to job applications
  - Write to people you want to work with, even if nothing is advertised
  - Don't waste time on pointless applications
- Play the long game
  - Prestige can be a means to an end
- Money matters
  - When interviewing for permanent/tenure track jobs, find out about the funding landscape in that country so you can talk about the grants you intend to apply for if you get the job