A stronger solution to Hilbert‘s Tenth Problem, and its *in-situ* formalization

Jonas Bayer and **Marco David**

A stronger solution to Hilbert‘s Tenth Problem, and its *in-situ* formalization

Jonas Bayer and **Marco David**

and Yuri Matiyasevich and Dierk Schleicher

A stronger solution to Hilbert‘s Tenth Problem, and its *in-situ* formalization

Jonas Bayer and **Marco David**

and Yuri Matiyasevich and Dierk Schleicher
and Malte Haßler and Thomas Serafini and Simon Dubischar

A stronger solution to Hilbert‘s Tenth Problem, and its *in-situ* formalization

Jonas Bayer and **Marco David**

and Yuri Matiyasevich and Dierk Schleicher
and Malte Haßler and Thomas Serafini and Simon Dubischar

and Timothé Ringeard and Xavier Pigé and Anna Danilkin and Mathis Bouverot-Dupuis and Paul Wang and Quentin Vermande and Theo André and Loïc Chevalier and Charlotte Dorneich and Eva Brenner and Chris Ye and Kevin Lee and Annie Yao

The Problem (1900)

Is there an algorithm to determine if a given Diophantine equation has a solution in the integers?

The Problem (1900)

Is there an algorithm to determine if a given Diophantine equation has a solution in the integers?

Parametric equation

$$a - y^2 = 0$$

The Problem (1900)

Is there an algorithm to determine if a given Diophantine equation has a solution in the integers?

Parametric equation

$$a - y^2 = 0$$

Parameter a

Unknown $y \in \mathbb{N}$

The Problem (1900)

Is there an algorithm to determine if a given Diophantine equation has a solution in the integers?

Parametric equation

$$a - y^2 = 0$$

Parameter a Unknown $y \in \mathbb{N}$

$\Longleftrightarrow$

Set of squares

1 49 4

0

16 25 ...

The OG Solution (1970)

Every recursively enumerable set is Diophantine.

The OG Solution (1970)

Every recursively enumerable set is Diophantine.

Hence, there is no algorithm that can decide all Diophantine equations.

The OG Solution (1970)

Every recursively enumerable set is Diophantine.

Hence, there is no algorithm that can decide all Diophantine equations.

More generally:

Hilbert Tenth's Problem over $\mathbb{Q}$?

The OG Solution (1970)

Every recursively enumerable set is Diophantine.

Hence, there is no algorithm that can decide all Diophantine equations.

More generally:

Hilbert Tenth's Problem over $\mathbb{Q}$?

More specifically:

Hilbert Tenth's Problem for bounded complexity ?

The OG Solution (1970)

Every recursively enumerable set is Diophantine.

Hence, there is no algorithm that can decide all Diophantine equations.

More generally:

Hilbert Tenth's Problem over $\mathbb{Q}$?

More specifically:

Hilbert Tenth's Problem for bounded complexity ?

DEF

$(\nu, \delta)_{\mathbb{N}}$ is a **universal pair** if any Diophantine set can be represented by a polynomial with i) at most ν unknowns in $\mathbb{N}$, ii) total degree at most δ.

Complicated Diophantine Equations

Is the set of primes Diophantine?

Complicated Diophantine Equations

Is the set of primes Diophantine?

Yes, primes are recursively enumerable. Explicitly:

$$
\begin{aligned}
(k+2)\Big\{1 &- [wz+h+j-q]^2 \\
&- [(gk+2g+k+1)(h+j)+h-z]^2 \\
&- [2n+p+q+z-e]^2 \\
&- \left[16(k+1)^3(k+2)(n+1)^2+1-f^2\right]^2 \\
&- \left[e^3(e+2)(a+1)^2+1-o^2\right]^2 \\
&- \left[(a^2-1)y^2+1-x^2\right]^2 \\
&- \left[16r^2y^4(a^2-1)+1-u^2\right]^2 \\
&- [n+l+v-y]^2 \\
&- \left[\left((a+u^2(u^2-a))^2-1\right)(n+4dy)^2+1-(x+cu)^2\right]^2 \\
&- \left[(a^2-1)l^2+1-m^2\right]^2 \\
&- \left[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x\right]^2 \\
&- \left[z+pl(a-p)+t(2ap-p^2-1)-pm\right]^2 \\
&- [ai+k+1-l-i]^2 \\
&- \left[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m\right]^2\Big\}.
\end{aligned}
$$

Complicated Diophantine Equations

Collatz Problem

$$f(n) = \begin{cases} \frac{n}{2}, & \text{if } n \text{ even} \\ 3n+1, & \text{else} \end{cases}$$

Complicated Diophantine Equations

Collatz Problem

$$f(n) = \begin{cases} \frac{n}{2}, & \text{if } n \text{ even} \\ 3n+1, & \text{else} \end{cases}$$

⇒ 36-page polynomial

Collatz Conjecture:
This polynomial encodes the Diophantine set $\mathbb{N}$.

Complicated Diophantine Equations

Collatz Problem

$$f(n) = \begin{cases} \frac{n}{2}, & \text{if } n \text{ even} \\ 3n+1, & \text{else} \end{cases}$$

$\Rightarrow$ 36-page polynomial

Collatz Conjecture:
This polynomial encodes the Diophantine set $\mathbb{N}$.

Other "Diophantine" Problems

– Goldbach Conjecture

– ABC Conjecture

– Riemann Hypothesis

Complicated Diophantine Equations

Collatz Problem

$$f(n) = \begin{cases} \frac{n}{2}, & \text{if } n \text{ even} \\ 3n+1, & \text{else} \end{cases}$$

$\Rightarrow$ 36-page polynomial

Collatz Conjecture:
This polynomial encodes the Diophantine set $\mathbb{N}$.

Other "Diophantine" Problems

- Goldbach Conjecture
- ABC Conjecture
- Riemann Hypothesis

? Given a Diophantine equation, can we find an equivalent, but simpler one?

Complicated Diophantine Equations

Collatz Problem

$$f(n) = \begin{cases} \frac{n}{2}, & \text{if } n \text{ even} \\ 3n+1, & \text{else} \end{cases}$$

$\Rightarrow$ 36-page polynomial

Collatz Conjecture:
This polynomial encodes the Diophantine set $\mathbb{N}$.

Other "Diophantine" Problems

– Goldbach Conjecture

– ABC Conjecture

– Riemann Hypothesis

DEF

$(\nu, \delta)_{\mathbb{N}}$ is a **universal pair** if any Diophantine set can be represented by a polynomial with i) at most ν unknowns in $\mathbb{N}$, ii) total degree at most δ.

Universal Pairs over $\mathbb{N}$ and $\mathbb{Z}$

$$a \geq 3$$

Universal Pairs over $\mathbb{N}$ and $\mathbb{Z}$

$$a \geq 3$$

$$\exists y \in \mathbb{N}.\, a = y + 3$$

Universal Pairs over $\mathbb{N}$ and $\mathbb{Z}$

$$a \geq 3$$

$$\exists y \in \mathbb{N}.\, a = y + 3$$

$$\exists x, y, z, w \in \mathbb{Z}.$$
$$a = (x^2 + y^2 + z^2 + w^2) + 3$$

Universal Pairs over $\mathbb{N}$ and $\mathbb{Z}$

$$a \geq 3$$

$$\exists y \in \mathbb{N}.\, a = y + 3$$

$$\exists x, y, z, w \in \mathbb{Z}.$$
$$a = (x^2 + y^2 + z^2 + w^2) + 3$$

Four Squares Theorem:
Any $n \in \mathbb{N}$ is given by
$$n = x^2 + y^2 + z^2 + w^2$$

Basic translation of pairs:

$$(\nu, \delta)_{\mathbb{N}} \implies (4\nu, 2\delta)_{\mathbb{Z}}$$

Universal Pairs over $\mathbb{N}$ and $\mathbb{Z}$

$$a \geq 3$$

$$\exists y \in \mathbb{N}.\, a = y + 3$$

$$\exists x, y, z, w \in \mathbb{Z}.$$
$$a = (x^2 + y^2 + z^2 + w^2) + 3$$

Four Squares Theorem:
Any $n \in \mathbb{N}$ is given by
$$n = x^2 + y^2 + z^2 + w^2$$

Basic translation of pairs:

$$(\nu, \delta)_{\mathbb{N}} \implies (4\nu, 2\delta)_{\mathbb{Z}}$$

Ex: $(58, 4)_{\mathbb{N}}$ $\quad (9, 1.64 \cdot 10^{45})_{\mathbb{N}}$

Universal Pairs over ℕ and ℤ

$$a \geq 3$$

$$\exists y \in \mathbb{N}.\, a = y + 3$$

$$\exists x, y, z, w \in \mathbb{Z}.$$
$$a = (x^2 + y^2 + z^2 + w^2) + 3$$

Four Squares Theorem:
Any $n \in \mathbb{N}$ is given by
$$n = x^2 + y^2 + z^2 + w^2$$

Basic translation of pairs:
$$(\nu, \delta)_{\mathbb{N}} \implies (4\nu, 2\delta)_{\mathbb{Z}}$$

Ex: $(58, 4)_{\mathbb{N}}$ $(9, 1.64 \cdot 10^{45})_{\mathbb{N}}$

! *For an axiomatizable theory T and any proposition P, if P has a proof in T, then P has another proof consisting of 100 additions and multiplications of integers.*

[Jones 1982]

First Nontrivial Universal Pair in $\mathbb{Z}$

THM

Let $(\nu, \delta)_{\mathbb{N}}$ be universal. Then

$$\big(11, \eta(\nu, \delta)\big)_{\mathbb{Z}}$$

is universal, where

$$\eta(\nu, \delta) = 15\,616 + 233\,856\,\delta + 233\,952\,\delta\,(2\delta + 1)^{\nu+1} + 467\,712\,\delta^2\,(2\delta + 1)^{\nu+1}.$$

COR

The pair

$$(11, 1\,681\,043\,235\,226\,619\,916\,301\,182\,624\,511\,918\,527\,834\,137\,733\,707\,408\,448\,335\,539\,840)$$

$$\approx (11, 1.68105 \cdot 10^{63})$$

is universal.

Optimizing universality

$$\begin{aligned}
\mathfrak{b}(a,f) &:= 1 + 3(2a+1)f \\
\mathcal{B}(a,f) &:= \beta\,\mathfrak{b}^{\delta} \\
M(a,f) &:= \mathrm{mask}(\mathfrak{b}, \mathcal{B}, \mathbf{n}) \\
N_0(a,f) &:= \mathcal{B}^{(\delta+1)^{\nu}+1} \\
N_1(a,f) &:= 4\mathcal{B}^{(2\delta+1)(\delta+1)^{\nu}+1} \\
N(a,f) &:= N_0 N_1 \\
c(a,f,g) &:= 1 + a\mathcal{B} + g \\
\mathcal{K}(a,f,g) &:= \mathrm{value}(c, \mathcal{B}) \\
\mathcal{S}(a,f,g) &:= g + 2\mathcal{K} N_0 \\
\mathcal{T}(a,f) &:= M + (\mathcal{B}-2)\mathcal{B}^{(\delta+1)^{\nu+1}} N_0 \\
\mathcal{R}(a,f,g) &:= (\mathcal{S}+\mathcal{T}+1)N + \mathcal{T} + 1 \\
\mathcal{X}(a,f,g) &:= (N-1)\mathcal{R} \\
\mathcal{Y}(a,f) &:= N^2
\end{aligned}$$

$$\begin{aligned}
U &:= 2lXY \\
V &:= 4gwY \\
A &:= U(V+1) \\
B &:= 2X+1 \\
C &:= B + (A-2)h \\
D &:= (A^2-4)C^2+4 \\
E &:= C^2 Dx \\
F &:= 4(A^2-4)E^2+1 \\
G &:= 1 + CDF - 2(A+2)(A-2)^2E^2 \\
H &:= C + BF + (2y-1)CF \\
I &:= (G^2-1)H^2+1 \\
J &:= X + 1 + k(U^2V-2)
\end{aligned}$$

$$\begin{aligned}
&DFI \in \square \\
&(U^4V^2-4)J^2+4 \in \square \\
&(2A-5) \mid (3bwC - 2(b^2w^2-1)) \\
&\left(\frac{C}{J} - lY\right)^2 < \frac{1}{16g^2}\,.
\end{aligned}$$

$$\begin{aligned}
A_1 &:= \mathfrak{b} \\
A_2 &:= DFI \\
A_3 &:= (U^4V^2-4)J^2+4 \\
S &:= 2A-5 \\
T &:= 3\mathfrak{b}wC - 2(\mathfrak{b}^2w^2-1)
\end{aligned}$$

Any chance Isabelle could help…?

The General Strategy

Given: Universal Pair $(\nu, \delta)_{\mathbb{N}}$ and a Diophantine Set A

$$a \in A$$

$$\Updownarrow$$

$$\exists y_1, \ldots, y_\nu \in \mathbb{N}^\nu : P_A(a, y_1, \ldots, y_\nu) = 0$$
$$\text{where } \deg P_A \leq \delta$$

$$\Updownarrow$$

…intermediate representations…

$$\Updownarrow$$

$$\exists y_1, \ldots, y_{11} \in \mathbb{Z}^{11} : P(a, y_1, \ldots, y_{11}) = 0$$
$$\text{where } \deg P \leq \eta(\nu, \delta)$$

Project Organisation

Core Student Workgroup at ENS Paris

Project Organisation

Core Student Workgroup at ENS Paris

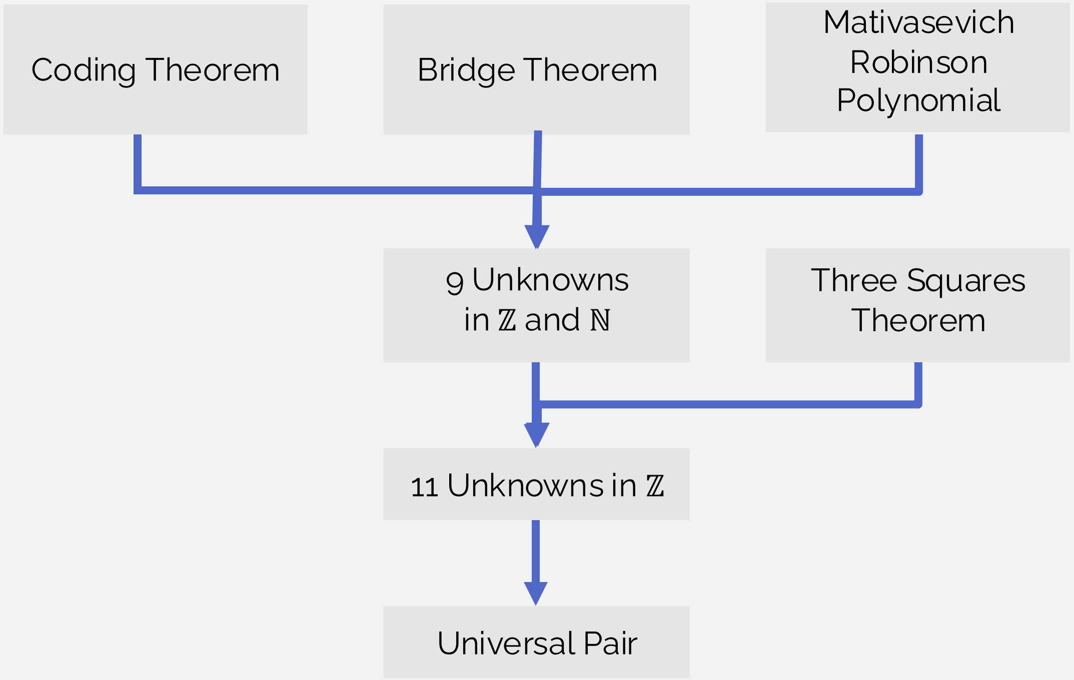
Isabelle workshop followed by throwing students in at the deep end

Project Organisation

Core Student Workgroup at ENS Paris

Isabelle workshop followed by throwing students in at the deep end

Structure of the mathematics emerged through formalisation



Polynomials in Isabelle

Isabelle datatype `mpoly` for multivariate polynomials

Example: `1 + 3 * (2 * Var 0 + 1) * Var 1`

Polynomials in Isabelle

Isabelle datatype `mpoly` for multivariate polynomials

Example: `1 + 3 * (2 * Var 0 + 1) * Var 1`

$$
\begin{aligned}
\mathfrak{b}(a,f) &:= 1 + 3(2a+1)f \\
\mathcal{B}(a,f) &:= \beta\,\mathfrak{b}^{\delta} \\
M(a,f) &:= \operatorname{mask}(\mathfrak{b}, \mathcal{B}, \mathbf{n}) \\
N_0(a,f) &:= \mathcal{B}^{(\delta+1)^{\nu}+1} \\
N_1(a,f) &:= 4\mathcal{B}^{(2\delta+1)(\delta+1)^{\nu}+1} \\
N(a,f) &:= N_0 N_1 \\
c(a,f,g) &:= 1 + a\mathcal{B} + g \\
\mathcal{K}(a,f,g) &:= \operatorname{value}(c, \mathcal{B}) \\
\mathcal{S}(a,f,g) &:= g + 2\mathcal{K}N_0 \\
\mathcal{T}(a,f) &:= M + (\mathcal{B}-2)\mathcal{B}^{(\delta+1)^{\nu+1}} N_0 \\
\mathcal{R}(a,f,g) &:= (\mathcal{S} + \mathcal{T} + 1)N + \mathcal{T} + 1 \\
\mathcal{X}(a,f,g) &:= (N-1)\mathcal{R} \\
\mathcal{Y}(a,f) &:= N^2
\end{aligned}
$$

Polynomials in Isabelle

Isabelle datatype `mpoly` for multivariate polynomials

Example: `1 + 3 * (2 * Var 0 + 1) * Var 1`

$$\begin{aligned}
\mathfrak{b}(a,f) &:= 1 + 3(2a+1)f \\
\mathcal{B}(a,f) &:= \beta\, \mathfrak{b}^{\delta} \\
M(a,f) &:= \mathrm{mask}(\mathfrak{b}, \mathcal{B}, \mathbf{n}) \\
N_0(a,f) &:= \mathcal{B}^{(\delta+1)^{\nu}+1} \\
N_1(a,f) &:= 4\mathcal{B}^{(2\delta+1)(\delta+1)^{\nu}+1} \\
N(a,f) &:= N_0 N_1 \\
c(a,f,g) &:= 1 + a\mathcal{B} + g \\
\mathcal{K}(a,f,g) &:= \mathrm{value}(c, \mathcal{B}) \\
\mathcal{S}(a,f,g) &:= g + 2\mathcal{K}N_0 \\
\mathcal{T}(a,f) &:= M + (\mathcal{B}-2)\mathcal{B}^{(\delta+1)^{\nu+1}} N_0 \\
\mathcal{R}(a,f,g) &:= (\mathcal{S}+\mathcal{T}+1)N + \mathcal{T} + 1 \\
\mathcal{X}(a,f,g) &:= (N-1)\mathcal{R} \\
\mathcal{Y}(a,f) &:= N^2
\end{aligned}$$

Command `poly_extract`

```
definition b :: "int ⇒ int ⇒ int" where
  "b a f ≡ 1 + 3*(2*a + 1) * f"

poly_extract b
```

```
consts
  b_poly :: "int mpoly"
Generated definition: 1 + 3 * (2 * Var 0 + 1) * Var 1
Proved correctness theorem: ⋀fn.
 insertion fn b_poly = coding_variables.b (fn 0) (fn 1)
```

Further command `poly_degree`

“In-situ” Formalisation

Formalized in its natural environment: A maths department

Manuscript & Formalisation developed at the same time

“In-situ” Formalisation

Formalized in its natural environment: A maths department

Manuscript & Formalisation developed at the same time

Benefits of the collaboration ITP <-> Researcher:

Fixing Bugs
Streamlining arguments
Precise Dependencies
Experimenting with the proof

“In-situ” Formalisation

Formalized in its natural environment: A maths department

Manuscript & Formalisation developed at the same time

Benefits of the collaboration ITP <-> Researcher:

Fixing Bugs
Streamlining arguments
Precise Dependencies
Experimenting with the proof

Isabelle works as a proof **assistant**

Future Work

Isabelle Feature Wishlist: Blueprint Tool

Future Work

Isabelle Feature Wishlist: Blueprint Tool

Means continuing the mathematical research!

- $2 \leq \nu \leq 10$?
- Universal Pairs for multiple parameters

Future Work

Isabelle Feature Wishlist: Blueprint Tool

Means continuing the mathematical research!

$2 \leq \nu \leq 10$?

Universal Pairs for multiple parameters

We unlock new research methods for researching extensions of Hilbert's Tenth Problem