Hilbert's tenth problem

Fanxin Wu

April 10, 2024

Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.* —David Hilbert

Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.* —David Hilbert

In modern language: is there an algorithm that determines whether a given (multivariate) polynomial with integer coefficients has any integer root?

Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.* —David Hilbert

In modern language: is there an algorithm that determines whether a given (multivariate) polynomial with integer coefficients has any integer root?

Theorem (Matiyasevich-Robinson-Davis-Putnam)

No.

Positive results

One variable: yes, easy.

Degree one: yes.

Degree two: yes, but very nontrivial; in particular it's decidable whether a given number can be written as $x^2 - ny^2$.

Positive results

One variable: yes, easy.

Degree one: yes.

Degree two: yes, but very nontrivial; in particular it's decidable whether a given number can be written as $x^2 - ny^2$.

Two variable: unknown.

Degree three: unknown.

Positive results

One variable: yes, easy.

Degree one: yes.

Degree two: yes, but very nontrivial; in particular it's decidable whether a given number can be written as $x^2 - ny^2$.

Two variable: unknown.

Degree three: unknown.

Degree four: as hard as general equation (Skolem), and thus undecidable by MRDP.

Sum of three cubes

For what n does $x^3 + y^3 + z^3 = n$ have integer solution? It is necessary that $n \neq \pm 4 \mod 9$; a folklore conjecture says this is also sufficient.

Sum of three cubes

For what n does $x^3 + y^3 + z^3 = n$ have integer solution? It is necessary that $n \neq \pm 4 \mod 9$; a folklore conjecture says this is also sufficient.

1955: Miller and Woollett used the EDSAC computer to find solution for all $n \leq 100$ (that are not $\pm 4 \mod 9$) except $n = 30, 33, 39, 42, 52, 74, 75, 84, 87$. They suggested maybe some of these are not sums of three cubes.

Sum of three cubes

For what n does $x^3 + y^3 + z^3 = n$ have integer solution? It is necessary that $n \neq \pm 4 \mod 9$; a folklore conjecture says this is also sufficient.

1955: Miller and Woollett used the EDSAC computer to find solution for all $n \leq 100$ (that are not $\pm 4 \mod 9$) except $n = 30, 33, 39, 42, 52, 74, 75, 84, 87$. They suggested maybe some of these are not sums of three cubes.

1964: computer search carried out for $1 < n \leq 1000$, $|y| \leq |x| \leq 65536$. For $n \leq 100$ the only new discovery was $87 = 4271^3 - 4126^3 - 1972^3$. The conclusion was that the conjecture is likely false.

Sum of three cubes

1955: Miller and Woollett used the EDSAC computer to find solution for all $n \leq 100$ (that are not $\pm 4 \mod 9$) except $n = 30, 33, 39, 42, 52, 74, 75, 84, 87$. They suggested maybe some of these are not sums of three cubes.

1964: computer search carried out for $1 < n \leq 1000$, $|y| \leq |x| \leq 65536$. For $n \leq 100$ the only new discovery was $87 = 4271^3 - 4126^3 - 1972^3$. The conclusion was that the conjecture is likely false.

1992-1995: solutions found for $n = 39, 75, 84$.

1999-2000: $n = 30, 52$.

Sum of three cubes

1964: computer search carried out for $1 < n \leq 1000$, $|y| \leq |x| \leq 65536$. For $n \leq 100$ the only new discovery was $87 = 4271^3 - 4126^3 - 1972^3$. The conclusion was that the conjecture is likely false.

1992-1995: solutions found for $n = 39, 75, 84$.

1999-2000: $n = 30, 52$.

2016: $n = 74$.

Sum of three cubes

1964: computer search carried out for $1 < n \leq 1000$, $|y| \leq |x| \leq 65536$. For $n \leq 100$ the only new discovery was $87 = 4271^3 - 4126^3 - 1972^3$. The conclusion was that the conjecture is likely false.

1992-1995: solutions found for $n = 39, 75, 84$.

1999-2000: $n = 30, 52$.

2016: $n = 74$.

2019: $n = 33, 42$.

Sum of three cubes

1964: computer search carried out for $1 < n \leq 1000$, $|y| \leq |x| \leq 65536$. For $n \leq 100$ the only new discovery was $87 = 4271^3 - 4126^3 - 1972^3$. The conclusion was that the conjecture is likely false.

1992-1995: solutions found for $n = 39, 75, 84$.

1999-2000: $n = 30, 52$.

2016: $n = 74$.

2019: $n = 33, 42$.

$33 = 8\ 866\ 128\ 975\ 287\ 528^3 + (-8\ 778\ 405\ 442\ 862\ 239)^3 + (-2\ 736\ 111\ 468\ 807\ 040)^3$

Diophantine equation

A simple observation: there is an algorithm deciding whether $f \in \mathbb{Z}[X_1, \ldots, X_n]$ has integer solution $\Leftrightarrow$ there is an algorithm deciding whether $f \in \mathbb{Z}[X_1, \ldots, X_n]$ has natural number solution.

Diophantine equation

A simple observation: there is an algorithm deciding whether $f \in \mathbb{Z}[X_1, \ldots, X_n]$ has integer solution $\Leftrightarrow$ there is an algorithm deciding whether $f \in \mathbb{Z}[X_1, \ldots, X_n]$ has natural number solution.

$\Rightarrow$: Lagrange's four-square theorem says every natural number is the sum of four squares of integers. So $f(X_1, \ldots, X_n)$ has natural number solution iff the following has integer solution.

$$f(X_{11}^2 + X_{12}^2 + X_{13}^2 + X_{14}^2, \ldots, X_{n1}^2 + X_{n2}^2 + X_{n3}^2 + X_{n4}^2)$$

Diophantine equation

A simple observation: there is an algorithm deciding whether $f \in \mathbb{Z}[X_1, \ldots, X_n]$ has integer solution $\Leftrightarrow$ there is an algorithm deciding whether $f \in \mathbb{Z}[X_1, \ldots, X_n]$ has natural number solution.

$\Rightarrow$: Lagrange's four-square theorem says every natural number is the sum of four squares of integers. So $f(X_1, \ldots, X_n)$ has natural number solution iff the following has integer solution.

$$f(X_{11}^2 + X_{12}^2 + X_{13}^2 + X_{14}^2, \ldots, X_{n1}^2 + X_{n2}^2 + X_{n3}^2 + X_{n4}^2)$$

$\Leftarrow$: For example, $f(X, Y)$ has integer solution iff one of $f(X, Y)$, $f(X, -Y)$, $f(-X, Y)$ and $f(-X, -Y)$ has natural number solution.

Diophantine equation

A subset of $\mathbb{N}^m$ is *Diophantine* if it is of the form

$\{\bar{a} \in \mathbb{N}^m : \exists \bar{x} \in \mathbb{N}^n \ f(\bar{a}, \bar{x}) = 0\}$

for some $f \in \mathbb{Z}[A_1, \ldots, A_m, X_1, \ldots, X_n]$

Diophantine equation

A subset of $\mathbb{N}^m$ is *Diophantine* if it is of the form

$\{\bar{a} \in \mathbb{N}^m : \exists \bar{x} \in \mathbb{N}^n \ f(\bar{a}, \bar{x}) = 0\}$

for some $f \in \mathbb{Z}[A_1, \ldots, A_m, X_1, \ldots, X_n]$

Theorem (Matiyasevich-Robinson-Davis-Putnam)

Diophantine sets are exactly the recursively enumerable sets.

Diophantine equation

A subset of $\mathbb{N}^m$ is *Diophantine* if it is of the form

$\{\bar{a} \in \mathbb{N}^m : \exists \bar{x} \in \mathbb{N}^n \; f(\bar{a}, \bar{x}) = 0\}$

for some $f \in \mathbb{Z}[A_1, \ldots, A_m, X_1, \ldots, X_n]$

Theorem (Matiyasevich-Robinson-Davis-Putnam)

Diophantine sets are exactly the recursively enumerable sets.

There is an r.e. set $S \subseteq \mathbb{N}^m$ that is not recursive. If S is defined by $f(\overline{A}, \overline{X})$, then there is no algorithm that determines whether $f(\bar{a}, \overline{X})$ has natural number solution for a given $\bar{a} \in \mathbb{N}^m$.

History of MRDP theorem

1949: Davis showed Diophantine sets are not closed under complementation.

1950: Robinson realized if there is a function such that: (i) its graph is Diophantine, (ii) it grows exponentially, then certain sets (such as the set of all primes) are Diophantine.

1959: Davis and Putnam improved Robinson's "certain sets" to all r.e. sets, conditional on the then unproven Green-Tao theorem.

1960: Robinson removed the dependence on Green-Tao.

1961-1969: People found various other reductions.

1970: Matiyasevich showed the function $n \mapsto F_{2n}$ works, where F_n is the n-th Fibonacci number.

Outline of the proof

We follow Lou's notes for the proof of MRDP theorem.

After some initial reductions, enough to show that Diophantine sets are closed under *bounded* universal quantification.

Outline of the proof

We follow Lou's notes for the proof of MRDP theorem.

After some initial reductions, enough to show that Diophantine sets are closed under *bounded* universal quantification.

This can be done if we assume $n \mapsto 2^n$ is Diophantine.

Outline of the proof

We follow Lou's notes for the proof of MRDP theorem.

After some initial reductions, enough to show that Diophantine sets are closed under *bounded* universal quantification.

This can be done if we assume $n \mapsto 2^n$ is Diophantine.

Define $x_a(n)$, $y_a(n)$ by $x_a(n) + y_a(n)\sqrt{a^2-1} = (a+\sqrt{a^2-1})^n$, i.e., $(x_a(n), y_a(n))$ is the n-th solution to he Pell's equation $x^2 - (a^2-1)y^2 = 1$.

Outline of the proof

We follow Lou's notes for the proof of MRDP theorem.

After some initial reductions, enough to show that Diophantine sets are closed under *bounded* universal quantification.

This can be done if we assume $n \mapsto 2^n$ is Diophantine.

Define $x_a(n)$, $y_a(n)$ by $x_a(n) + y_a(n)\sqrt{a^2-1} = (a+\sqrt{a^2-1})^n$, i.e., $(x_a(n), y_a(n))$ is the n-th solution to he Pell's equation $x^2 - (a^2-1)y^2 = 1$.

Use intricate congruence properties of these numbers to show $(a,n) \mapsto y_a(n)$ is Diophantine, which in turn implies that $n \mapsto 2^n$ is Diophantine.

Basic properties

Convention: polynomials $f(\overline{X})$ have integer coefficients; variables $a, b, c, x, y, z, m, n, u, \dots$ range over natural numbers.

A Diophantine set is of form $\{\bar{a} : \exists \bar{x}\ f(\bar{a}, \bar{x}) = 0\}$.

Basic properties

Convention: polynomials $f(\overline{X})$ have integer coefficients; variables $a, b, c, x, y, z, m, n, u, \ldots$ range over natural numbers.

A Diophantine set is of form $\{\bar{a} : \exists \bar{x}\ f(\bar{a}, \bar{x}) = 0\}$.

Examples:

- $\{(a, b) : a < b\} \subseteq \mathbb{N}^2$ is Diophantine: $\exists x\ a + x + 1 - b = 0$.
- $\{(a, b) : a \mid b\} \subseteq \mathbb{N}^2$ is Diophantine: $\exists x\ a \cdot x - b = 0$
- $\{(a, b, c) : a \equiv b \mod c\} \subseteq \mathbb{N}^3$ is Diophantine: $\exists x\ (a - b - cx) \cdot (b - a - cx) = 0$.

Basic properties

Diophantine sets are closed under union and intersection: consider $f \cdot g$ and $f^2 + g^2$ resp.

A function is Diophantine if its graph is. $\gcd(a, b)$ and $\mathrm{rem}(a, b)$ are Diophantine. For $\gcd(a, b)$ consider $\exists x \exists y\ (ax - by = c \vee by - ax = c) \wedge c \mid a \wedge c \mid b$.

Diophantine functions are closed under composition. Preimage or image of Diophantine set under Diophantine function is Diophantine.

Basic properties

Since $\leq$, $\wedge$ and $\vee$ are Diophantine, any set defined by $\exists \bar{x} \varphi$, where φ is quantifier-free, is Diophantine.

Basic properties

Since $\leq$, $\wedge$ and $\vee$ are Diophantine, any set defined by $\exists \bar{x} \varphi$, where φ is quantifier-free, is Diophantine.

Recall that r.e. sets are defined by $\exists \bar{x} \varphi$ where φ is bounded. To show that r.e. sets are Diophantine, it suffices to show that Diophantine sets are closed under bounded universal quantification. To show this we temporarily assume that $n \mapsto 2^n$ is Diophantine.

Basic properties

Since $\leq$, $\wedge$ and $\vee$ are Diophantine, any set defined by $\exists \bar{x} \varphi$, where φ is quantifier-free, is Diophantine.

Recall that r.e. sets are defined by $\exists \bar{x} \varphi$ where φ is bounded. To show that r.e. sets are Diophantine, it suffices to show that Diophantine sets are closed under bounded universal quantification. To show this we temporarily assume that $n \mapsto 2^n$ is Diophantine.

Lemma: If 2^x is Diophantine, so are x^y, $\binom{x}{y}$ and $x!$.

Basic properties

Since $\leq$, $\wedge$ and $\vee$ are Diophantine, any set defined by $\exists \bar{x} \varphi$, where φ is quantifier-free, is Diophantine.

Recall that r.e. sets are defined by $\exists \bar{x} \varphi$ where φ is bounded. To show that r.e. sets are Diophantine, it suffices to show that Diophantine sets are closed under bounded universal quantification. To show this we temporarily assume that $n \mapsto 2^n$ is Diophantine.

Lemma: If 2^x is Diophantine, so are x^y, $\binom{x}{y}$ and $x!$.

$2^{xy} \equiv x \mod 2^{xy} - x$

$2^{xy^2} \equiv x^y \mod 2^{xy} - x$

$x^y = \mathrm{rem}(2^{xy^2}, 2^{xy} - x)$ if $y > 1$ (since $x^y < 2^{xy} - x$)

Bounded quantification theorem

A small further reduction: we want to show a set of form

$\forall u \leq x \exists \bar{v}\ F(\bar{a}, x, u, \bar{v}) = 0$

is Diophantine, where
$F(\overline{A}, X, U, \overline{V}) \in \mathbb{Z}[A_1, \ldots, A_m, X, U, V_1, \ldots, V_n]$.

Bounded quantification theorem

A small further reduction: we want to show a set of form

$\forall u \leq x \exists \bar{v}\ F(\bar{a}, x, u, \bar{v}) = 0$

is Diophantine, where
$F(\overline{A}, X, U, \overline{V}) \in \mathbb{Z}[A_1, \ldots, A_m, X, U, V_1, \ldots, V_n]$.

Note that

$\forall u \leq x \exists \bar{v}\ F(\bar{a}, x, u, \bar{v}) = 0 \Leftrightarrow \exists y \forall u \leq x \exists \bar{v} \leq y\ F(\bar{a}, x, u, \bar{v}) = 0$

Enough to show $\forall u \leq x \exists \bar{v} \leq y\ F(\bar{a}, x, y, u, \bar{v}) = 0$ is Diophantine.

Bounded quantification theorem

A small further reduction: we want to show a set of form

$$\forall u \leq x \exists \bar{v}\ F(\bar{a}, x, u, \bar{v}) = 0$$

is Diophantine, where
$F(\overline{A}, X, U, \overline{V}) \in \mathbb{Z}[A_1, \ldots, A_m, X, U, V_1, \ldots, V_n]$.

Note that

$$\forall u \leq x \exists \bar{v}\ F(\bar{a}, x, u, \bar{v}) = 0 \Leftrightarrow \exists y \forall u \leq x \exists \bar{v} \leq y\ F(\bar{a}, x, u, \bar{v}) = 0$$

Enough to show $\forall u \leq x \exists \bar{v} \leq y\ F(\bar{a}, x, y, u, \bar{v}) = 0$ is Diophantine.

For simplicity assume $n = 1$.

Bounded quantification theorem

$$\forall u \leq x \exists v \leq y \; F(\bar{a}, x, y, u, v) = 0$$

$$F(\overline{A}, X, Y, U, V) \in \mathbb{Z}[A_1, \ldots, A_m, X, Y, U, V].$$

Bounded quantification theorem

$$\forall u \leq x \exists v \leq y \; F(\bar{a}, x, y, u, v) = 0$$

$$F(\overline{A}, X, Y, U, V) \in \mathbb{Z}[A_1, \ldots, A_m, X, Y, U, V].$$

Idea: this holds iff there are b and coprime p_u's for $u \leq x$ s.t. $\mathrm{rem}(b, p_u) \leq y$ and $F(\bar{a}, x, y, u, \mathrm{rem}(b, p_u)) = 0$.

Bounded quantification theorem

$$\forall u \leq x \exists v \leq y \; F(\bar{a}, x, y, u, v) = 0$$

$$F(\overline{A}, X, Y, U, V) \in \mathbb{Z}[A_1, \ldots, A_m, X, Y, U, V].$$

Idea: this holds iff there are b and coprime p_u's for $u \leq x$ s.t. $\mathrm{rem}(b, p_u) \leq y$ and $F(\bar{a}, x, y, u, \mathrm{rem}(b, p_u)) = 0$.

To express this for all $u \leq x$, find a large number M s.t. $M \equiv u \mod p_u$, and the above implies

$$F(\bar{a}, x, y, M, b) \equiv 0 \mod \prod_{u \leq x} p_u.$$

Bounded quantification theorem

$$\forall u \le x \exists v \le y \; F(\bar{a}, x, y, u, v) = 0$$

$$F(\overline{A}, X, Y, U, V) \in \mathbb{Z}[A_1, \ldots, A_m, X, Y, U, V].$$

Idea: this holds iff there are b and coprime p_u's for $u \le x$ s.t. $\mathrm{rem}(b, p_u) \le y$ and $F(\bar{a}, x, y, u, \mathrm{rem}(b, p_u)) = 0$.

To express this for all $u \le x$, find a large number M s.t. $M \equiv u \mod p_u$, and the above implies

$F(\bar{a}, x, y, M, b) \equiv 0 \mod \prod_{u \le x} p_u$.

Choose p_u carefully plus some other stuff to make this sufficient.

Bounded quantification theorem

$$\forall u \leq x \exists v \leq y \; F(\bar{a}, x, y, u, v) = 0$$

$$F(\overline{A}, X, Y, U, V) \in \mathbb{Z}[A_1, \ldots, A_m, X, Y, U, V].$$

Bounded quantification theorem

$$\forall u \leq x \exists v \leq y \; F(\bar{a}, x, y, u, v) = 0$$

$$F(\overline{A}, X, Y, U, V) \in \mathbb{Z}[A_1, \ldots, A_m, X, Y, U, V].$$

Choose $G(\overline{A}, X, Y)$ s.t. $G(\bar{a}, x, y) > 2x + 2$, $G(\bar{a}, x, y) > y + 1$, and $G(\bar{a}, x, y) > |F(\bar{a}, x, y, u, v)|$ for all $u \leq x$ and $v \leq y$. E.g., let $G(\overline{A}, X, Y) = F^*(\overline{A}, X, Y, X, Y) + 2X + Y + 3$ where F^* replaces all coefficients in F by absolute values.

Bounded quantification theorem

$$\forall u \le x \exists v \le y \; F(\bar{a}, x, y, u, v) = 0$$

$$F(\overline{A}, X, Y, U, V) \in \mathbb{Z}[A_1, \ldots, A_m, X, Y, U, V].$$

Choose $G(\overline{A}, X, Y)$ s.t. $G(\bar{a}, x, y) > 2x + 2$, $G(\bar{a}, x, y) > y + 1$, and $G(\bar{a}, x, y) > |F(\bar{a}, x, y, u, v)|$ for all $u \le x$ and $v \le y$. E.g., let $G(\overline{A}, X, Y) = F^*(\overline{A}, X, Y, X, Y) + 2X + Y + 3$ where F^* replaces all coefficients in F by absolute values.

BQT: $\forall u \le x \exists v \le y \; F(\bar{a}, x, y, u, v) = 0 \Leftrightarrow$
$\exists b \left[\binom{b}{y+1} \equiv F(\bar{a}, x, y, g! - 1, b) \equiv 0 \mod \binom{g! - 1}{x+1} \right]$

where $g = G(\bar{a}, x, y)$.

Bounded quantification theorem

Let $g = G(\bar{a}, x, y)$, then $\forall u \leq x \exists v \leq y \; F(\bar{a}, x, y, u, v) = 0 \Leftrightarrow$
$\exists b \left[\binom{b}{y+1} \equiv F(\bar{a}, x, y, g! - 1, b) \equiv 0 \mod \binom{g!-1}{x+1} \right]$

Bounded quantification theorem

Let $g = G(\bar{a}, x, y)$, then $\forall u \leq x \exists v \leq y \; F(\bar{a}, x, y, u, v) = 0 \Leftrightarrow$
$\exists b \left[\binom{b}{y+1} \equiv F(\bar{a}, x, y, g! - 1, b) \equiv 0 \mod \binom{g!-1}{x+1} \right]$

$$\binom{g!-1}{x+1} = \frac{(g!-1)(g!-2)\cdots(g!-x-1)}{1 \cdot 2 \cdots (x+1)}$$
$$= \frac{g!-1}{1} \cdot \frac{g!-2}{2} \cdots \frac{g!-x-1}{x+1}$$
$$= \left(\frac{g!}{1} - 1\right) \cdot \left(\frac{g!}{2} - 1\right) \cdots \left(\frac{g!}{x+1} - 1\right)$$

Claim: each prime factor of $\binom{g!-1}{x+1}$ is $> g$, and $\frac{g!}{u+1} - 1$ are coprime.

Bounded quantification theorem

Let $g = G(\bar{a}, x, y)$, then $\forall u \leq x \exists v \leq y \; F(\bar{a}, x, y, u, v) = 0 \Leftrightarrow$
$\exists b \left[\binom{b}{y+1} \equiv F(\bar{a}, x, y, g! - 1, b) \equiv 0 \mod \binom{g!-1}{x+1} \right]$

$$\binom{g!-1}{x+1} = \frac{(g!-1)(g!-2)\cdots(g!-x-1)}{1 \cdot 2 \cdots (x+1)}$$
$$= \frac{g!-1}{1} \cdot \frac{g!-2}{2} \cdots \frac{g!-x-1}{x+1}$$
$$= \left(\frac{g!}{1} - 1\right) \cdot \left(\frac{g!}{2} - 1\right) \cdots \left(\frac{g!}{x+1} - 1\right)$$

Claim: each prime factor of $\binom{g!-1}{x+1}$ is $> g$, and $\frac{g!}{u+1} - 1$ are coprime.

For each $u \leq x$ let p_u be a prime factor of $\frac{g!}{u+1} - 1$. So $g! - 1 \equiv u \mod p_u$, and for any b we have
$F(\bar{a}, x, y, g! - 1, b) \equiv F(\bar{a}, x, y, u, \mathrm{rem}(b, p_u)) \mod p_u$

Bounded quantification theorem

Let $g = G(\bar{a}, x, y)$, then $\forall u \leq x \exists v \leq y \; F(\bar{a}, x, y, u, v) = 0 \Leftrightarrow$
$\exists b \left[\binom{b}{y+1} \equiv F(\bar{a}, x, y, g! - 1, b) \equiv 0 \mod \binom{g! - 1}{x+1} \right]$

$\Leftarrow$: Suppose such a b exists, in particular $p_u \mid \binom{b}{y+1}$ for each $u \leq x$, so $p_u \mid b \cdot (b-1) \cdots (b-y)$, so $p_u \mid (b-k)$ for some $k \leq y$. Thus $\mathrm{rem}(b, p_u) \leq y$, and by assumption on g we have

$$|F(\bar{a}, x, y, u, \mathrm{rem}(b, p_u))| < g < p_u,$$

but this is also congruent mod p_u to $F(\bar{a}, x, y, g! - 1, b)$, so it's 0.

Bounded quantification theorem

Let $g = G(\bar{a}, x, y)$, then $\forall u \leq x \exists v \leq y \; F(\bar{a}, x, y, u, v) = 0 \Leftrightarrow$
$\exists b \left[\binom{b}{y+1} \equiv F(\bar{a}, x, y, g! - 1, b) \equiv 0 \mod \binom{g!-1}{x+1} \right]$

$\Rightarrow$: Suppose for every $u \leq x$ there exists such a $v_u \leq y$. By CRT there is a $b < \binom{g!-1}{x+1}$ s.t. $\operatorname{rem}(b, \frac{g!}{u+1} - 1) = v_u$. Thus

$\frac{g!}{u+1} - 1 \mid (b - v_u) \mid b \cdot (b-1) \cdots (b-y)$

Then $\binom{g!-1}{x+1} \mid \binom{b}{y+1}$ since each prime factor of $\binom{g!-1}{x+1}$ is $> g$ and $g > y + 1$. Also easy to check $g! - 1 \equiv u \mod \frac{g!}{u+1} - 1$, so $F(\bar{a}, x, y, g! - 1, b) \equiv 0 \mod \frac{g!}{u+1} - 1$ for each $u \leq x$, and the result follows.

Pell's equation

It remains to show $n \mapsto 2^n$ is Diophantine. For this we use the properties of Pell's equation

$$x^2 - dy^2 = 1$$

$(x, y) \in \mathbb{N}^2$ is a solution iff $x + y\sqrt{d}$ is a unit in the ring $O_{\mathbb{Q}(\sqrt{d})}$; if $x_1 + y_1\sqrt{d}$ and $x_2 + y_2\sqrt{d}$ are units then so is their product, so $(x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1)$ is a solution.

The Indian mathematician Bhāskara II (c. 1114–1185) was the first to show that there always exist nontrivial solutions. In modern language, the group of units of $O_{\mathbb{Q}(\sqrt{d})}$ is isomorphic to $\{-1, 1\} \times \mathbb{Z}$, and the generator for $\mathbb{Z}$ is the element $x + y\sqrt{d}$ with $x > 1$ minimal.

Pell's equation

The minimal solution to Pell's equation varies wildly, e.g., when $d = 61$ it's $x = 1766319049,\ y = 226153980$, due to Fermat.

We are going to consider the family $x^2 - (a^2 - 1)y^2 = 1$, whose minimal solution is obviously $(a, 1)$. Define $x_a(n)$, $y_a(n)$ by

$$x_a(n) + y_a(n)\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^n$$

Pell's equation

The minimal solution to Pell's equation varies wildly, e.g., when $d = 61$ it's $x = 1766319049,\ y = 226153980$, due to Fermat.

We are going to consider the family $x^2 - (a^2 - 1)y^2 = 1$, whose minimal solution is obviously $(a, 1)$. Define $x_a(n)$, $y_a(n)$ by

$$x_a(n) + y_a(n)\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^n$$

They satisfy various formulas, such as

$$y_a(m + n) = x_a(m)y_a(n) + x_a(n)y_a(m)$$

$$y_a(n + 2) = 2ay_a(n + 1) - y_a(n)$$

Pell's equation

Growth rate: $(2a-1)^n \leq y_a(n+1) < (2a)^2$, $2n \leq y_a(n)$ for $n \geq 2$

Congruence rules: $y_a(n) \equiv n \mod a-1$,
$y_a(n) \equiv y_b(n) \mod a-b$

Periodicity: if $y_a(n) \equiv 0 \mod m$ then $y_a(k) \equiv y_a(l) \mod m$ for any $k = l \mod 2n$

1st step-down lemma: $y_a(m) \mid y_a(n) \Leftrightarrow m \mid n$
$y_a(m)^2 \mid y_a(n) \Leftrightarrow my_a(m) \mid n$

2nd step-down lemma: if $y_a(k) \equiv y_a(l) \mod x_a(n)$ then $k \equiv \pm l \mod 2n$

Pell's equation

Claim: for $a, y, n \geq 2$, we have $y = y_a(n)$ iff there are x, u, v, s, t, b such that

(i) $2n \leq y$
(ii) $x^2 - (a^2 - 1)y^2 = 1$
(iii) $v \geq 1$ & $u^2 - (a^2 - 1)v^2 = 1$
(iv) $b \geq 2$ & $s^2 - (b^2 - 1)t^2 = 1$
(v) $b \equiv a \mod u$
(vi) $b \equiv 1 \mod y$
(vii) $t \equiv y \mod u$
(viii) $t \equiv n \mod y$
(ix) $y^2 \mid v$

Pell's equation

Claim: for $a, y, n \geq 2$, we have $y = y_a(n)$ iff there are x, u, v, s, t, b such that

(i) $2n \leq y$
(ii) $x^2 - (a^2 - 1)y^2 = 1$
(iii) $v \geq 1$ & $u^2 - (a^2 - 1)v^2 = 1$
(iv) $b \geq 2$ & $s^2 - (b^2 - 1)t^2 = 1$
(v) $b \equiv a \mod u$
(vi) $b \equiv 1 \mod y$
(vii) $t \equiv y \mod u$
(viii) $t \equiv n \mod y$
(ix) $y^2 \mid v$

Idea?: (ii) implies $y = y_a(k)$ for some k. By the growth bound we have $2k \leq y$, and some intricate (but completely elementary) arguments show $n \equiv \pm k \mod y$.

Exponentiation is Diophantine

$$(2a-1)^n \le y_a(n+1) < (2a)^2, \quad (4a-1)^n \le y_{2a}(n+1) < (4a)^2$$

Exponentiation is Diophantine

$$(2a-1)^n \leq y_a(n+1) < (2a)^2, \quad (4a-1)^n \leq y_{2a}(n+1) < (4a)^2$$

$$\frac{(4a-1)^n}{(2a)^n} \leq \frac{y_{2a}(n+1)}{y_a(n+1)} \leq \frac{(4a)^n}{(2a-1)^n}$$

$$2^n\left(1-\frac{1}{4a}\right)^n \leq \frac{y_{2a}(n+1)}{y_a(n+1)} \leq 2^n\left(1+\frac{1}{2a-1}\right)^n$$

Exponentiation is Diophantine

$$(2a-1)^n \le y_a(n+1) < (2a)^2, \quad (4a-1)^n \le y_{2a}(n+1) < (4a)^2$$

$$\frac{(4a-1)^n}{(2a)^n} \le \frac{y_{2a}(n+1)}{y_a(n+1)} \le \frac{(4a)^n}{(2a-1)^n}$$

$$2^n\left(1-\frac{1}{4a}\right)^n \le \frac{y_{2a}(n+1)}{y_a(n+1)} \le 2^n\left(1+\frac{1}{2a-1}\right)^n$$

Some simple estimation shows if $a \ge 2ny_3(n+1)+1$ then

$$\left|\frac{y_{2a}(n+1)}{y_a(n+1)} - 2^n\right| < \frac{1}{2},$$

so $2^n = m \Leftrightarrow 2|y_{2a}(n+1) - my_a(n+1)| < y_a(n+1)$

Variants

One can also ask about solutions in other rings or fields. The theories of $\mathbb{Q}_p$, $\mathbb{R}$ and $\mathbb{C}$ are decidable, so there exist algorithm for checking, e.g., whether a given polynomial with integer coefficients has real solution.

Variants

One can also ask about solutions in other rings or fields. The theories of $\mathbb{Q}_p$, $\mathbb{R}$ and $\mathbb{C}$ are decidable, so there exist algorithm for checking, e.g., whether a given polynomial with integer coefficients has real solution.

MRDP extends to many (but currently not all) number rings.

Variants

One can also ask about solutions in other rings or fields. The theories of $\mathbb{Q}_p$, $\mathbb{R}$ and $\mathbb{C}$ are decidable, so there exist algorithm for checking, e.g., whether a given polynomial with integer coefficients has real solution.

MRDP extends to many (but currently not all) number rings.

An important open case is Hilbert tenth for rationals. Robinson proved in 1949 that $\mathbb{Z}$ is definable in $\mathbb{Q}$, using a formula of form $\forall\bar{x}\exists\bar{y}\forall\bar{z} f(n, \bar{x}, \bar{y}, \bar{z}) = 0$. Consequently, the theory of $\mathbb{Q}$ is undecidable.

Poonen improved this to $\forall\exists$, and Koenigsmann found a $\forall$-definition. If there is an $\exists$-definition then Hilbert tenth for rationals would have a negative answer, but this is impossible assuming the Bombieri-Lang conjecture in number theory.

Reference

Recursion Theory, Lou van den Dries, online notes

A Course in Mathematical Logic, Yuri Manin

Undecidability in number theory, Bjorn Poonen, online notes