HILBERT'S TENTH PROBLEM

SHILIN LAI

Abstract. Hilbert's tenth problem asks for a "process" to decide if a Diophantine equation has integer solutions. This turned out to be impossible by the works of Davis–Putnam–Robinson and Matiyasevich. The talk will start with a basic introduction to computation theory, formalizing the notion of "process". It will then sketch the main ideas of the negative solution to Hilbert's tenth problem, which shows the much stronger conclusion that in some sense, Diophantine equations can simulate all computations.

This is the expanded version of the notes for my talk given at the Princeton Graduate Students' Seminar. We follow the survey article [Dav73], except rearranging its content to better reflect the history of the solution.

0. Background

Most of number theory began with the study of a problem of the following form:

"Given a polynomial $P(x_1, \cdots, x_n)$ with integer coefficients, does it have integer roots?"

Hilbert's tenth problem asks for a general procedure to solve this problem. Note that he did not ask if such a procedure exists: there was no formal notion of an undecidable problem, and there might not have been the expectation that such a problem existed. In fact, Hilbert later proposed the more ambitious Entscheidungsproblem, which asked for a general procedure to decide the validity of *any* (first-order) mathematical statement. From a modern point of view at least, this is too good to exist.

In the 1930s, Church and Turing independently proposed models of computation and showed that the Entscheidungsproblem cannot be solved. The theorem of Davis–Putnam–Robinson–Matiyasevich is that even when restricted to the class of Diophantine equations, there is still no decision algorithm, which seems plausible once one accept that undecidable problems exist.

1. Computability

We will think of a computation problem as a partial function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$, where $k \in \mathbb{N}$ is the number of inputs. For the purpose of this talk, $0 \in \mathbb{N}$. Further recall that a common notation for $\underline{n} \notin \mathrm{dom}(f)$ is $f(\underline{n})\uparrow$. It is useful to think that $f(\underline{n})\uparrow$ corresponds to a computation which does not terminate.

Let $\mathcal{P}_k$ be the set of all partial functions $\mathbb{N}^k \dashrightarrow \mathbb{N}$ and $\mathcal{P}_\omega = \bigcup_{k\geq 0} \mathcal{P}_k$. A model of computation specifies a subset of $\mathcal{P}_\omega$ as the computable functions. The model we will use is the subset of recursive functions

Definition 1. The set $\mathcal{R}$ of *(partial) recursive functions* is the smallest subset of $\mathcal{P}_\omega$ such that

Basic functions: The following functions are in $\mathcal{R}$:

- $\mathtt{zero} : \mathbb{N} \to \mathbb{N},\ n \mapsto 0$
- $\mathtt{succ} : \mathbb{N} \to \mathbb{N},\ n \mapsto n + 1$
- $\mathtt{pr}_{i,k} : \mathbb{N}^k \to \mathbb{N},\ (n_1, \cdots, n_k) \mapsto n_i$

Composition: If $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ and $g_1, \cdots, g_k : \mathbb{N}^l \dashrightarrow \mathbb{N}$ are all in $\mathcal{R}$, then so is

$$f \circ (g_1, \cdots, g_k) : \mathbb{N}^l \dashrightarrow \mathbb{N},\ \underline{n} \mapsto f(g_1(\underline{n}), \cdots, g_k(\underline{n}))$$

Primitive recursion: If $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ and $g : \mathbb{N}^{k+2} \dashrightarrow \mathbb{N}$ are both in $\mathcal{R}$, then so is

$$\mathtt{rec}_{f,g} : \mathbb{N}^{k+1} \dashrightarrow \mathbb{N},\ (\underline{n}, n_{k+1}) \mapsto \begin{cases} f(\underline{n}) & \text{if } n_{k+1} = 0 \\ g(\underline{n}, n_{k+1}, \mathtt{rec}_{f,g}(\underline{n}, n_{k+1} - 1)) & \text{otherwise} \end{cases}$$

Unbounded minimization: If $f : \mathbb{N}^{k+1} \dashrightarrow \mathbb{N}$ is in $\mathcal{R}$, then so is

$$\mu_f : \mathbb{N}^k \dashrightarrow \mathbb{N},\ \underline{n} \mapsto \begin{cases} m & \text{if } f(\underline{n}, m) = 0 \text{ and } f(\underline{n}, m') > 0 \text{ for all } m' < m \\ \uparrow & \text{otherwise} \end{cases}$$

Remark. If unbounded minimization is not allowed, then the resulting functions are called *primitive recursive*. They are all total functions. When intersected with $\mathcal{P}_1$, they are the "slowly-growing" ones among all total recursive functions.

Functions in $\mathcal{R}$ obviously should be computable by any reasonable definition. Conversely, we have the following vague statement

Church–Turing Thesis. *Any reasonable definition of computability can only produce functions in $\mathcal{R}$.*

Another model of computation is the Turing machine, which more closely resembles a typical procedural programming language. One of the observations which led to the Church–Turing thesis was that $\mathcal{R}$ is exactly the set of functions that can be computed on a Turing machine. This is not conceptually hard to prove, but it is very technical. We will later encounter some ideas which were used in its proof. For now, here is a very basic example of constructing recursive functions.

Example 2. The following is a prototype for conditional expressions. Given $f : \mathbb{N} \to \mathbb{N}$ which is known to be total, define

$$\mathtt{if}_f : \mathbb{N} \dashrightarrow \mathbb{N},\ n \mapsto \begin{cases} 1 & \text{if } f(n) = 0 \\ 0 & \text{otherwise} \end{cases}$$

If f is computable, then $\mathtt{if}_f$ should also be computable. Indeed, define $g : \mathbb{N} \to \mathbb{N}$ using primitive recursion by $g(0) = 1,\ g(n+1) = \mathtt{zero}(n)$, then $\mathtt{if}_f = g \circ f$.

From now on, to describe a function in $\mathcal{R}$, we will only describe an algorithm in the intuitive sense. For each such algorithm, it is theoretically easy to write down the proper description showing that it is in $\mathcal{R}$.

Definition 3. Let $S \subseteq \mathbb{N}^k$.

- If the function
$$\mathtt{E}_S : \mathbb{N}^k \dashrightarrow \mathbb{N},\ \underline{n} \mapsto \begin{cases} 0 & \text{if } \underline{n} \in S \\ \uparrow & \text{if } \underline{n} \notin S \end{cases}$$
is in $\mathcal{R}$, then S is *recursively enumerable/semi-decidable*.
- If the function
$$\mathtt{I}_S : \mathbb{N}^k \dashrightarrow \mathbb{N},\ \underline{n} \mapsto \begin{cases} 1 & \text{if } \underline{n} \in S \\ 0 & \text{if } \underline{n} \notin S \end{cases}$$
is in $\mathcal{R}$, then S is *decidable/computable*.

Remark. An equivalent condition for being recursively enumerable is that there exists an algorithm which, when given $n \in \mathbb{N}$ as an input, outputs the n-th member of S, ordered by size. This explains its name.

Example 4.

- The set of primes is decidable by the Church–Turing thesis.
- Exercise: decidable sets are semi-decidable.
  Harder exercise: $S \subseteq \mathbb{N}^k$ is decidable if and only if S and $\mathbb{N}^k \backslash S$ are both semi-decidable.
- **Key example**: Let $P \in \mathbb{Z}[a_1, \cdots, a_n, x_1, \cdots, x_m]$. Think of $a_1, \cdots, a_n$ as parameters and $x_1, \cdots, x_m$ as variables. Define its solvable set
$$\mathtt{sol}_P = \{(a_1, \cdots, a_n) \in \mathbb{N}^n \mid (\exists x_1, \cdots, x_m \in \mathbb{N})(P(a_1, \cdots, a_n, x_1, \cdots, x_m) = 0)\}$$
where by abuse of notation we do not mark the parameters.

  For each P, $\mathtt{sol}_P$ is semi-decidable. Indeed, fix a computable listing of $\mathbb{N}^m$, then given $a_1, \cdots, a_m$, test each element of the list to see if the Diophantine equation is satisfied. The key point is that if $(a_1, \cdots, a_m) \in \mathtt{sol}_P$, then the process terminates, and otherwise the process does not, which is represented by undefined value.

  If Hilbert's tenth problem has a solution, then $\mathtt{sol}_P$ is decidable for all P. This does not follow immediately from definition since Hilbert's tenth problem asks for solutions in $\mathbb{Z}$, as opposed to $\mathbb{N}$. To fix this, replace each x_i with $\sum_{j=1}^4 y_{ij}^2$ and observe that every natural number is a sum of four integer squares.

The following theorem is arguably the foundational result of computation theory

Theorem 5 (Church, Turing)**.** *Not all semi-decidable sets are decidable.*

Proof. This is a consequence of the celebrated theorem that the halting problem is undecidable. The proof uses the diagonal argument, which we informally sketch now.

First observe that $\mathcal{R} \cap \mathcal{P}_1$ is countable, and in fact there exists an algorithm listing its elements. Let φ_n be the n-th function in this list. We define the halting set

$$\mathbb{H} = \{n \mid \varphi_n(n) \text{ is defined}\}$$

This is semi-decidable, since $\mathtt{E}_{\mathbb{H}} = \mathtt{zero} \circ (n \mapsto \varphi_n(n))$. Suppose $\mathbb{N}\backslash\mathbb{H}$ is semi-decidable, then there exists n such that $\varphi_n = \mathtt{E}_{\mathbb{N}\backslash\mathbb{H}}$. Evaluate both sides at n. If $\varphi_n(n)$ is defined, then $n \in \mathbb{H}$, so $\mathtt{E}_{\mathbb{N}\backslash\mathbb{H}}$ is undefined. Conversely, if $\varphi_n(n)$ is undefined, then $\mathtt{E}_{\mathbb{N}\backslash\mathbb{H}} = 0$ is defined. This is a contradiction, so $\mathbb{N}\backslash\mathbb{H}$ is not semi-decidable. It follows that $\mathbb{H}$ is not decidable. □

With the appropriate definitions at hand, we can state the main theorem.

Theorem 6 (Davis–Putnam–Robinson–Matiyasevich)**.** *If $S \subseteq \mathbb{N}^n$ is semi-decidable, then there exists a polynomial P such that $\mathtt{sol}_P = S$. In particular, Hilbert's tenth problem has no solution.*

Corollary 7. *There exists a Diophantine equation which has a solution if and only if* ZFC *is inconsistent.*

2. Normal forms

From now, all quantifiers are over $\mathbb{N}$.

Definition 8.

- A set $S \subseteq \mathbb{N}^n$ is *Diophantine* if it is $\mathtt{sol}_P$ for some P.
- A function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ is Diophantine if the graph of f (namely the set $\{(\underline{n}, f(\underline{n})) \mid \underline{n} \in \mathrm{dom}(f)\}$) is Diophantine.

The goal is therefore to prove that the semi-decidable sets are all Diophantine. Observe that syntactically, Diophantine sets take the form

$$\{\underline{a} \in \mathbb{N}^n \mid (\exists x_1, \cdots, x_m)(P(\underline{a}, \underline{x}) = 0)\}$$

We call predicates of the form $P(\underline{x}) = 0$ *polynomial predicates*. Another way of phrasing the main theorem is that all semi-decidable sets can be formed by existential quantifiers applied to a polynomial predicate.

The proof has two steps: first prove a weaker normal form statement allowing more logical operations, in particular including universal quantifiers; then show that all operations involved are Diophantine-constructible. But universal quantifiers are not inherently computable, since they involve checking an infinite number of cases, so we must restrict them to be bounded.

Definition 9. The set of *bounded elementary predicates* is the smallest subset of all first-order predicates containing all polynomial predicates and closed under $\wedge$, $\vee$, existential quantifier $(\exists x)$, and bounded universal quantifier $(\forall_{<y} x) := (\forall x)((y \geq x) \vee -)$.

Observe that all Diophantine predicates are bounded elementary.

Theorem 10 (Davis)**.** *Any semi-decidable set can be defined using a bounded elementary predicate.*

Proof. This is Lemma 4 in Section 3 of [Dav53], where it is proven as a corollary to works of Gödel and Kleene. The proof applies structural induction to show that the graphs of all recursive functions can be put into the required form, i.e. given a recursive function $f : \mathbb{N}^n \dashrightarrow \mathbb{N}$, there exists a bounded elementary predicate P_f of arity $n+1$ such that $P(\underline{x}, y) \iff f(\underline{x}) = y$. This is enough: suppose $S \subseteq \mathbb{N}^n$ and $\mathrm{Graph}(\mathtt{E}_S)$ is defined by $R(\underline{x}, y)$, then S is defined by $(\exists y)R(\underline{x}, y)$.

The basic functions are obvious. For example, the projection $\mathtt{proj}_{1,2}$ is defined by the polynomial predicate $a_1 - a_3 = 0$, with variables a_1, a_2, a_3. For composition, to save notations, we will consider the case of $f : \mathbb{N}^2 \dashrightarrow \mathbb{N}$ and $g_1, g_2 : \mathbb{N} \dashrightarrow \mathbb{N}$. Suppose $P(a_1, a_2, a_3)$ is a bounded elementary predicate defining f, $Q_1(\alpha_1, \alpha_2)$ defines g_1, and $Q_2(\beta_1, \beta_2)$ defines g_2, then $f \circ (g_1, g_2)$ can be defined by

$$R(\alpha, \beta) := (\exists u, v)(Q_1(\alpha, u) \wedge Q_2(\alpha, v) \wedge P(u, v, \beta))$$

For bounded minimization, suppose $P(\underline{a}, b, c)$ defines the function $f : \mathbb{N}^{n+1} \dashrightarrow \mathbb{N}$, then

$$\mu_P(\underline{a}, c) := P(\underline{a}, c, 0) \wedge (\forall_{<c} u)(\exists x) P(\underline{a}, u, x+1)$$

is a predicate defining μ_f.

Recursion is much more difficult. Suppose $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ and $g : \mathbb{N}^{k+2} \dashrightarrow \mathbb{N}$ are defined by bounded elementary predicates $P(\underline{x}, v)$ and $Q(\underline{x}, y, z, v)$ respectively. The idea is that we keep track of the entire history of the recursion in a sequence, which yields the following

$$v = \mathtt{rec}_{f,g}(\underline{x}, y) \iff (\exists s \in \mathbb{N}^{y+1})\big(P(\underline{x}, s_0) \wedge (\forall_{<y} z) Q(\underline{x}, z+1, s_z, s_{z+1}) \wedge s_{z+1} = v\big)$$

This is not a first-order predicate, since we cannot qualify over sequences of indefinite length. To solve this issue, we use the device of Gödel numbering. More precisely, to a pair of natural numbers (n, p), we can attach a sequence $s^{(n,p)}$ whose k-th term is $n \pmod{1+(k+1)p}$. Gödel showed using the Chinese remainder theorem that for any *finite* sequence, there exists $(n, p) \in \mathbb{N}^2$ such that $s^{(n,p)}$ agrees with it. The integer n will be called the Gödel code for the sequence (note that it depends on p). Moreover, the condition $s_k^{(n,p)} = x$ is equivalent to

$$(x < 1 + (k+1)p) \wedge (\exists d)(n - x = d(1 + (k+1)p))$$

which is Diophantine. Therefore, after replacing the quantifier $(\exists s \in \mathbb{N}^{y+1})$ by $(\exists n, p \in \mathbb{N})$ and a predicate of the form $R(s_z)$ by $(\exists \alpha)(s_k^{(n,p)} = \alpha \wedge R(\alpha))$, we get a bounded elementary definition of $\mathtt{rec}_{f,g}$. □

Remark. By extending the above proof, the expressions can be simplified further to

$$\{\underline{a} \in \mathbb{N}^n \mid (\exists y)(\forall_{<y} k)(\exists x_1, \cdots, x_m)(P(\underline{a}, k, y, x_1, \cdots, x_m) = 0)\}$$

This is the Davis normal form, which was used in the first arrangement of the proof of the DPRM theorem.

Therefore, it remains to emulate the operations $\wedge$, $\vee$, $(\exists x)$, and $(\forall_{\le y} x)$. The first two are easy: if $S_i = \mathtt{sol}_{P_i}$ for $i = 1, 2$, then

$$S_1 \cap S_2 = \mathtt{sol}_{P_1^2 + P_2^2}, \quad S_1 \cup S_2 = \mathtt{sol}_{P_1 P_2}$$

The existential quantifier is part of the Diophantine language. What remains is the bounded universal quantifier, i.e. we need to prove the following statement: let P be a polynomial, then

$$\{(\underline{a}, y) \in \mathbb{N}^{n+1} \mid (\forall_{<y} z)(\exists \underline{x} \in \mathbb{N}^m)(P(\underline{a}, y, z, \underline{x}) = 0)\}$$

is Diophantine. Its proof is divided into two parts: first, Davis–Putnam–Robinson [DPR61] showed that the statement is true if we allow variables in the exponents; then Matiyasevich [Mat70] showed, based on earlier works of Robinson [Rob52], that exponentiation is Diophantine.

3. Exponential Diophantine equations

For a fixed polynomial P as before, we need to define

$$B(\underline{a}, y) := \bigwedge_{z=0}^{y-1} \big((\exists \underline{x} \in \mathbb{N}^m)(P(\underline{a}, y, z, \underline{x}) = 0)\big)$$

The idea is to use Gödel numbering. Suppose $R(\underline{a}, y)$ holds, then for each variable x_i, we get a sequence $x_i^{(z)}$, $0 \le z < y$ such that $P(\underline{a}, y, z, \underline{x}^{(z)}) = 0$. Let X_i be a Gödel code for $(x_i^{(z)})_z$ described earlier, and let Z be a Gödel code for $(0, 1, \cdots, y-1)$. Since z-th terms of all sequences are extracted by taking remainders modulo the same number, we can hope that an equation of the form $P(\underline{a}, y, Z, \underline{X}) \equiv 0 \pmod{M}$ for a really large modulus M is equivalent to the disjunction of the y equations. It is clear that M should grow exponentially in y, which was why exponential Diophantine equations are needed.

To make the discussion more precise, first make the trivial observation that for fixed $\underline{a}$ and y, if $R(\underline{a}, y)$ holds, then there exists a bound on all variables in a solution, since there are only finitely many of them. Conversely, if there are bounded solutions, then there are solutions. Therefore,

$$B(\underline{a}, y) \iff (\exists u)(\forall_{<y} z)(\exists_{\le u} \underline{x} \in \mathbb{N}^m)(P(\underline{a}, y, z, \underline{x}) = 0)$$

The point is that in the predicate inside $(\exists u)$, all variables appearing have an a priori bound.

Let $R(\underline{a}, y, u)$ be the polynomial obtained from P by taking absolute value of all coefficients of P, replacing every z with y, and replacing every x_i with u. Let $Q(\underline{a}, y, u) = R(\underline{a}, y, u) + y + u + 1$. It is clear that

(1) $Q(\underline{a}, y, u) > y, u$.
(2) $|P(\underline{a}, y, z, \underline{x})| \leq Q(\underline{a}, y, u)$ if $0 \leq x_i \leq u$ and $z \leq y$.

This is an upper bound on all possible values of P. Now consider the following big predicate

$$(\exists Z, t)(\exists \underline{X} \in \mathbb{N}^m)\Big(1 + (Z+1)t = \prod_{z=0}^{y-1}(1+(z+1)t) \wedge t = \prod_{l=1}^{Q(\underline{a},y,u)} l$$
$$\wedge \bigwedge_{k=1}^{m}\Big((1+(Z+1)t)\Big|\prod_{j=0}^{u}(X_k - j)\Big)$$
$$\wedge (1+(Z+1)t)|P(\underline{a}, y, Z, \underline{X})\Big)$$

This is equivalent to $(\forall_{<y} z)(\exists_{\leq u}\underline{x} \in \mathbb{N}^m)(P(\underline{a}, y, z, \underline{x}) = 0)$, the predicate of $B(\underline{a}, y)$ inside of $(\exists u)$. Indeed, by thinking of $\underline{X}$ and Z as Gödel codes introduced earlier, we can define

$$s_z^{(Z,t)} = Z \pmod{1+(z+1)t},\ x_i^{(z)} := s_z^{(X_i,t)} = X_i \pmod{1+(z+1)t}$$

The second term forces t to be sufficiently large and divisible for the argument to work. The first term gives $s_z^{(Z,t)} = z$. The third term forces $x_i^{(z)} \leq u$ for all $z < y$ and $k \leq m$. By the Chinese remainder theorem, the first and last term of the big predicate together are equivalent to $P(\underline{a}, y, z, \underline{x}^{(z)}) \equiv 0 \pmod{1+(z+1)t}$ for each z, which, by the choice of Q, implies that $P(\underline{a}, y, z, \underline{x}^{(z)}) = 0$.

We have therefore eliminated the bounded universal quantifier, at the cost of introducing the construction $y = \prod_{k=1}^{x}(a+bk)$. The technical heart of [DPR61] is to show that this relation can be defined using exponential Diophantine equations. First observe that

$$\prod_{k=1}^{x}(a+bk) = \binom{a/b+x}{x} b^x x!$$

Choose M to be larger than the left hand side and coprime to b, say $M = b(a+bx)^x + 1$. Working modulo M, we may replace $\frac{a}{b}$ by the minimal non-negative solution to $a = qb \pmod{M}$, reducing the problem to the construction of the following two functions

$$x = n!, \quad x = \binom{n}{k}$$

Finally, observe the following identities

$$\binom{n}{k} \equiv \left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor \pmod{u}, \quad n! = \left\lfloor r^n / \binom{r}{n} \right\rfloor$$

if $u > 2^n$ and $r > (2n)^{n+1}$. They are not hard to prove. Now, the relation $x = \lfloor \frac{p}{q} \rfloor$ is equivalent to $(qx \leq p) \wedge (q(x+1) > p)$, which is Diophantine. Therefore, the above identities can be used to give the required exponential Diophantine representations.

4. Diophantine definition of exponentiation

This is the final step of the proof. The goal is to define the relation $x = y^z$ using Diophantine equations. The proof is very technical, and finally, there is some number theory involved, namely the description of solutions of the Pell equation.

Definition 11. Let $a > 1$ and $n \geq 0$, then define $(p(n,a), q(n,a))$ by

$$p(n,a) + q(n,a)\sqrt{a^2-1} = (a + \sqrt{a^2-1})^n$$

The following proposition contains some classical properties of the two sequences.

Proposition 12.

(1) The only non-negative integer solutions to $x^2 - (a^2-1)y^2 = 1$ are of the form $(p(n,a), q(n,a))$ for some $n \geq 0$.
(2) $q(n,a) \equiv n \pmod{a-1}$.
(3) If $y > 1$ and $a > y^z$, then $y^z = \lfloor p(z, ay)/p(z,a) \rfloor$

To use these fact to represent exponentiation, we first need to find a Diophantine predicate which represents at least exponential growth. This is done starting from the Pell equation by imposing congruence conditions on $q(n,a)$. Define

$$\psi(a,v) := (\exists p,q)\big((p^2-(a^2-1)(a-1)^2q^2=1)\wedge(p,a>1)\wedge v=ap\big)$$

A solution to the first equation has the form $(p(n,a),q(n,a))$ with the additional constraint that $(a-1)|q(n,a)$, which implies $(a-1)|n$ by (2). Therefore, if $\psi(a,v)$ holds, then $v\geq ap(a-1,a)\geq a^a$. Now by the growth property of ψ and (3), the predicate

$$(\exists a,b,c)((x<a)\wedge(y,z<b)\wedge\psi(b,c)\wedge(c<a)\wedge x=\lfloor p(z,ay)/p(z,y)\rfloor)$$

represents $x=y^z$ up to some trivial cases which can be coded explicitly. Therefore, it remains to prove that the function $p(n,a)$ is Diophantine. This is the contribution of Matiyasevich [Mat70].

Theorem 13 (Matiyasevich)**.** *Consider the following system of Diophantine equations:*

$$x^2-(a^2-1)y^2=1 \tag{1}$$
$$u^2-(a^2-1)v^2=1 \tag{2}$$
$$s^2-(b^2-1)t^2=1 \tag{3}$$
$$v=ry^2 \tag{4}$$
$$b=1+4py=a+qu \tag{5}$$
$$s=x+(c+1)u \tag{6}$$
$$t=n+4dy \tag{7}$$
$$y=n+e \tag{8}$$

Given $(a,x,n)\in\mathbb{N}^2$ with $a>1$, it can be solved in the other 12 variables if and only if $x=p(n,a)$.

Proof. Exercise. In [Mat93], the author gave some indications of his thought process when he discovered the equations. The key point is that congruence properties (beyond what was stated above) are used to access the index n. □

References

[Dav53] Martin Davis. Arithmetical problems and recursively enumerable predicates. *J. Symbolic Logic*, 18:33–41, 1953.

[Dav73] Martin Davis. Hilbert's tenth problem is unsolvable. *Amer. Math. Monthly*, 80:233–269, 1973.

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson. The decision problem for exponential diophantine equations. *Ann. of Math. (2)*, 74:425–436, 1961.

[Mat70] Ju. V. Matijasevič. The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191:279–282, 1970.

[Mat93] Yuri V. Matiyasevich. *Hilbert's tenth problem*. Foundations of Computing Series. MIT Press, Cambridge, MA, 1993. Translated from the 1993 Russian original by the author, With a foreword by Martin Davis.

[Rob52] Julia Robinson. Existential definability in arithmetic. *Trans. Amer. Math. Soc.*, 72:437–449, 1952.