Diophantine Sets, Primes, and the Resolution of Hilbert's 10th Problem

Lawrence Cabusora

April 5, 2004

1 Introduction

The term *recursively enumerable set* has its roots in logic but today is most commonly seen in reference to the theory of Turing machines. The Turing machine model is conceptually a very simple one for an abstract computing device but has been proved to be so powerful that many believe that that which is "computable" or "recursive" in any reasonable sense of the word is computable by some Turing machine; this is commonly known as Church's Thesis.

For the purposes of our discussion, we need only sketch the model: A Turing machine consists of an infinite tape with discrete "squares," and a read/write head that can move left and right along the tape as well as read and write symbols in the squares on the tape. The rules that the head is allowed to use can only direct it to either write a new symbol on the tape or move precisely one square to the left or right. A Turing machine may reach a "halting state" – in this case, the machine simply stops – or it may operate indefinitely without ever reaching such a state.

It is this last condition that gives rise to the notion of a recursively enumerable set. We can set a canonical method for representing a tuple $(x_1, \ldots, x_n)$ using symbols on a Turing machine tape, then "program" the head with rules that allow it to calculate based on this input. Then we say that a set E is recursively enumerable if there exists some Turing machine that, given $(x_1, \ldots, x_n)$ as input, will eventually halt if and only if $(x_1, \ldots, x_n) \in E$. (The name "recursively enumerable" comes from the fact that any such set can actually be "enumerated" by a Turing machine by successively printing out all of its members onto the tape.)

The Turing machine model was proposed and developed in the 1930's by Alan Turing, Alonzo Church, and Kurt Gödel; they formulated the first rigorous definitions of the formerly intuitive notions of algorithm and computability. In doing so, they constructed the foundations upon which #10 of Hilbert's 23 outstanding mathematical problems would eventually be solved. Thirty years before the concept of the Turing machine had been published, Hilbert had phrased the problem as follows:

> 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.

We will examine the slight variation on Hilbert's tenth problem that was attacked until its solution in 1970 by Yuri Matiyasevich. That is, we will consider the term "Diophantine equation" to refer to a polynomial equation in which all the coefficients are integers; then the problem becomes whether it is possible to find an algorithm for determining the solubility of Diophantine equations when its variables range over the integers.

The development of the theory of Turing machiens was cotemperaneous with Gödel's development of the notion of *primitive recursive functions*, which he was using in his incompleteness results. The primitive recursive functions are built up from a very small set of basic functions:

$$\begin{aligned} \text{suc} &: \mathbb{Z}^+ \to \mathbb{Z}^+, x \mapsto x+1 \\ 1^{(n)} &: (\mathbb{Z}^+)^n \to \mathbb{Z}^+, (x_1, \ldots, x_n) \mapsto 1 \\ \text{pr}_i^n &: (\mathbb{Z}^+)^n \to \mathbb{Z}^+, (x_1, \ldots, x_n) \mapsto x_i \end{aligned}$$

("pr" is short for "projection." The idea of extracting specific coordinates from a tuple, in effect projecting the tuple onto those coordinates, will become particularly important later.)

The primitive recursive functions are then constructed by closing the set of basic functions under the finite application of the following operations: composition, juxtaposition, and recursion. *Composition* denotes the usual mathematical sense of the word. Given functions f, g taking $(x_1, \ldots, x_n)$ to $(y_1, \ldots, y_p), (z_1, \ldots, z_q)$, respectively, *juxtaposition* allows us to define a new function $h : (\mathbb{Z}^+)^n \to (\mathbb{Z}^+)^p \times (\mathbb{Z}^+)^q, (x_1, \ldots, x_n) \mapsto (y_1, \ldots, y_p, z_1, \ldots, z_q)$. *Recursion*—actually, primitive recursion, but unless otherwise specified, that is what "recursion" will mean throughout this paper—is the most complicated operation and gives this definition most of its potency: Given $f : (\mathbb{Z}^+)^n \to \mathbb{Z}^+$ and $g : (\mathbb{Z}^+)^{n+2} \to \mathbb{Z}^+$, applying recursion lets us define $h : (\mathbb{Z}^+)^{n+1} \to \mathbb{Z}^+, (x_1, \ldots, x_n, 1) \mapsto f(x_1, \ldots, x_n), (x_1, \ldots, x_n, k+1) \mapsto g(x_1, \ldots, x_n, k, h(x_1, \ldots, x_n, k))$. (Hence, f serves as the initial condition, and g gives us the recursive calculation.)

A great deal of the familiar functions on the positive integers are primitive recursive; we will use the term *PRF* for such functions. For example, addition is a PRF because if we take f to be suc and g to be $\text{suc} \circ \text{pr}_3^3$, then the function defined by recursion using f and g is precisely addition. Multiplication can be obtained from recursion on addition, then exponentiation from recursion on multiplication. This highlights the important fact that, given known PRFs, any application of the composition, juxtaposition, and recursion operations to them will yield another PRF. (We note that in many presentations of this subject matter, juxtaposition is not included in the definition of a PRF. This is simply because these presentations initially only concern themselves with PRFs whose range $\subseteq \mathbb{Z}^+$, and defer discussion of higher dimensions.)

The PRFs do not cover all of the functions on the positive integers that we might consider computable. For example, the Ackermann function is a natural example of a computable function that is not primitive recursive. To encompass all such functions, the class of "general recursive" functions is defined by adding an operation called the μ-operator whose intuitive effect is to introduce partial functions (specifically, from a function $f : (\mathbb{Z}^+)^n \to \mathbb{Z}^+$, the μ-operator defines $g : (\mathbb{Z}^+)^{n-1} \to \mathbb{Z}^+$ such that $g(x_1, \ldots, x_{n-1}) = \min\{x_n \mid f(x_1, \ldots, x_{n-1}, x_n) = 1\}$; clearly, there is no guarantee that g will be everywhere-defined for arbitrary f). Given the details of a Turing machine formalism, it then becomes relatively simple to show the following connection between recursively enumerable sets $\subseteq (\mathbb{Z}^+)^n$ (as we defined them earlier) and general recursive functions: E is recursively enumerable if and only if

$$E = \{(x_1, \ldots, x_n) \in (\mathbb{Z}^+)^n \mid \exists y_1, \ldots, y_m \in \mathbb{Z}^+, [f(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]\}$$

for some general recursive function f. Equivalently, the level set of any recursive function is the range of some other recursive function. (See [Soare] for details.)

One surprising associated fact is that if we replace the phrase "general recursive function" by "primitive recursive function" in the above statement, the result continues to hold. This in itself is a very interesting result; however, we will not touch on the proof here. (Details can be found in many books on recursion theory, for example, [Soare]. Also see [Kleene].)

The even more surprising result for which Matiyasevich's work completed the proof was the fact that the further "reduction" of substituting the words "polynomial with coefficients $\in \mathbb{Z}$" for "primitive recursive function" in the above result *still* does not change the class of sets thus defined. In other words, any recursively enumerable set is the projection (to certain of its coordinates) of the 0-level set of some polynomial with integer coefficients.

As stated earlier, such a polynomial is called a Diophantine polynomial. A subset of $(\mathbb{Z}^+)^n$ which can be shown to be equal to $\{(x_1, \ldots, x_n) \in (\mathbb{Z}^+)^n \mid \exists y_1, \ldots, y_m \in \mathbb{Z}^+, [f(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]\}$ for some Diophantine polynomial f is then called a Diophantine set. Finally, the terminology is extended to include relations and functions, since any relation can be represented naturally by a set, namely its graph. For example, $<$ is a Diophantine relation since $a < b \iff (a, b) \in \{(x_1, x_2) \in (\mathbb{Z}^+)^2 \mid \exists y \in \mathbb{Z}^+, [x_1 + y - x_2 = 0]\}$ and $x_1 + y - x_2$ is a Diophantine polynomial in the (x_1, x_2, y) space.

We note that the basic PRFs are Diophantine; we exhibit the relevant polynomial equations:

$$\begin{aligned} y = \mathrm{suc}(x) &\iff y - x - 1 = 0 \\ y = 1^{(n)}(x_1, \ldots, x_n) &\iff y - 1 = 0 \\ y = \mathrm{pr}_i^n(x_1, \ldots, x_n) &\iff x_i - y = 0 \end{aligned}$$

The result that the class of r.e. sets is identical with the class of Diophantine sets implies the insolubility of Hilbert's tenth problem, as we now explain. First, we show that the Diophantine sets can be "Diophantically enumerated": since all polynomials with positive integral coefficients can be built up from 1 and variables by repeated addition and multiplication, it is possible to enumerate every such polynomial in a list $\mathbf{P}_0, \mathbf{P}_1, \mathbf{P}_2, \cdots$ (for details, see [Davis1973]). Now, we have defined Diophantine sets (of positive integers) as those which can be represented $\{y \in \mathbb{Z}^+ \mid \exists x_1, \ldots, x_n, [f(x_1, \ldots, x_m, y) = 0]\}$ for some polynomial f with coefficients $\in \mathbb{Z}$. This trivially is the same as the class of sets that can be represented $\{y \in \mathbb{Z}^+ \mid \exists x_1, \ldots, x_m, [\mathbf{P}_i(x_1, \ldots, x_m, y) = \mathbf{P}_j(x_1, \ldots, x_m, y)]\}$ for some $\mathbf{P}_i, \mathbf{P}_j$ as defined above.

To encode the pairs $(i, j) \in (\mathbb{Z}^+)^2$ into a single number $n \in \mathbb{Z}^+$, we can use the function $\mathrm{pair}(i, j) = (i + j - 1)(i + j - 2)/2 + j$. Then left$(n)$ can be Diophantically defined by the i such that $\exists j, [2n = (i + j - 1)(i + j - 2) + 2j]$ and similarly for right(n). Thus, $D_n = \{y \in \mathbb{Z}^+ \mid \exists x_1, \ldots, x_m, [\mathbf{P}_{\mathrm{left}(n)}(x_1, \ldots, x_m, y) = \mathbf{P}_{\mathrm{right}(n)}(x_1, \ldots, x_m, y)]\}$ is an enumeration of all of the Diophantine sets; moreover, it can be defined in a Diophantine fashion.

We apply Cantor's diagonal method to the D_n's: let $V = \{n \mid n \notin D_n\}$. V cannot be Diophantine; otherwise, it would be equal to D_n for some n, then n cannot logically be either $\in D_n$ or $\notin D_n$. On the other hand, as mentioned above, "$z \in D_n$" is a Diophantine relation, so there is some polynomial f with coefficients $\in \mathbb{Z}^+$ with the property $z \in D_n \iff (n, z) \in \{(y_1, y_2) \in (\mathbb{Z}^+)^2 \mid \exists x_1, \ldots, x_m, [f(x_1, \ldots, x_m, y_1, y_2) = 0]\}$. Now suppose Hilbert's tenth problem were soluble, and there was an algorithm to tell whether arbitrary Diophantine equations had positive integer solutions or not. In particular, this algorithm would be able to calculate, for any n, whether $f(x_1, \ldots, x_m, n, n) = 0$ has a solution, i.e., whether $n \in D_n$ or, more importantly, $n \notin D_n$. Since Turing machines can perform all algorithms (assuming we accept Church's thesis), we can design a Turing machine that on input n will halt if and only if $n \notin D_n$. By the Turing machine definition of recursively enumerable, this means that $V = \{n \mid n \notin D_n\}$ is an r.e. set. But if we know that all r.e. sets are Diophantine, this means that V is Diophantine, and we already showed that it cannot be. This is a contradiction, so Hilbert's tenth problem is insoluble.

The actual result that Matiyasevich proved was that a certain relation with "roughly" exponential growth (in fact, $v = \phi_{2u}$, where ϕ_n denotes the nth Fibonacci number) was Diophantine. It had previously been proved by Julia Robinson that if any coordinate of a Diophantine relation

could be shown to exhibit exponential growth with respect to all the other coordinates, then exponentiation itself was Diophantine. This, in turn, combined with the results of Robinson, Martin Davis, and Hilary Putnam in [Davis1961] to show that the class of r.e. sets is identical with the class of Diophantine sets.

The next two sections will be devoted to showing a proof that is a variation on that original line of investigation. Much of the framework is borrowed from [Manin]; the proof will also use many simplifications from later works of Matiyasevich, Robinson, and Davis.

2 D-sets and the bounded universal quantifier

We first define some ground notions. Note that unless otherwise specified, all variables are to be taken to be from $\mathbb{Z}^+$. (Should we wish to refer to the set of natural numbers including 0, we shall use the notation $\mathbb{N}$.) Recall: a set F is *Diophantine* if there is some polynomial f with coefficients $\in \mathbb{Z}$ such that $F = \{(x_1, \ldots, x_n) \mid \exists y_1, \ldots, y_m, [f(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]\}$. F is *recursively enumerable* (abbr. "r.e") if there is a primitive recursive function g such that $F = \{(x_1, \ldots, x_n) \mid \exists y_1, \ldots, y_m, [g(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]\}$.

To show that these two classes are in fact one and the same, we introduce what Manin calls the class of "D-sets" (probably after Martin Davis; the notion is nearly the same as that of Davis Normal Form expressions). To define this, we need an operator called the *bounded universal quantifier*, defined as follows: Given a set F whose members are of the form $(x_1, \ldots, x_n)$, the set G is said to be obtained by bounded universal quantification on the ith coordinate if $(x_1, \ldots, x_i, \ldots, x_n) \in F \iff \forall k, [1 \leq k \leq x_i \implies (x_1, \ldots, x_{i-1}, k, x_{i+1}, \ldots, x_n) \in G]$.

The class of *D-sets* is obtained from the class of Diophantine sets by closing it under the operations of finite direct product, finite union, finite intersection, finite direct product, projection, and application of the bounded universal quantifier. The overall plan of proof, then, is to show that the class of recursively enumerable sets is the same as the class of D-sets and to subsequently prove that the class of D-sets coincides with the class of Diophantine sets. We start with proving that {r.e. sets} = {D-sets}.

The r.e. sets are closed under union, intersection, direct product, and projection: Take E_1, E_2, E_3 to be r.e. sets defined by PRFs $f_1 : (\mathbb{Z}^+)^{n+p} \to \mathbb{Z}^+, f_2 : (\mathbb{Z}^+)^{n+q} \to \mathbb{Z}^+, f_3 : (\mathbb{Z}^+)^{m+r} \to \mathbb{Z}^+$, respectively, i.e.,

$$E_1 = \{x = (x_1, \ldots, x_n) \mid \exists y = (y_1, \ldots, y_p), [f_1(x, y) = 0]\},$$

and similarly for E_2, a set of n-tuples and E_3, a set of m-tuples. (We use the shorthand $f(x, y)$ for "$f(x_1, \ldots, x_n, y_1, \ldots, y_p)$".)

Let x and y denote n- and p-tuples as above, and let z, u, v denote q-, m-, r-tuples. Then $E_1 \cap E_2$ is the projection of the 0-level set of the function $g(x, y, z) = (f_1(x, y))^2 + (f_2(x, z))^2$ onto its first n coordinates, and $E_1 \cup E_2$ is the projection of the 0-level set of the $g(x, y, z) = f_1(x, y) \cdot f_2(x, z)$ onto its first n coordinates. $E_1 \times E_3$ is the projection of the 0-level set of $g(x, u, y, v) = (f_1(x, y))^2 + (f_3(u, v))^2$ onto its first $n + m$ coordinates. These are all PRFs, so each set is r.e. (Closure under projection follows immediately from the definition.)

Any D-set can be obtained from Diophantine sets through the previously mentioned operations, and {Diophantine sets} $\subseteq$ {r.e sets} (because every polynomial is primitive recursive). We have just shown the closure of {r.e. sets} under all of the operations except bounded universal quantification; if we can show closure for that, then we will have proved that {D-sets} $\subseteq$ {r.e. sets}.

Proposition: {r.e. sets} is closed under bounded universal quantification.

Proof: We start with r.e. set E, a projection of the 0-level set of PRF f onto its first n coordinates. Let F be the set obtained from E by bounded universal quantification on the nth coordinate: $(x_1, \ldots, x_n) \in F \iff$ for $1 \leq k \leq x_n$, $\exists y_{1k}, \ldots, y_{mk}$ such that $f(x_1, \ldots, x_{n-1}, k, y_{1k}, \ldots . y_{mk}) = 0$. We want a PRF g such that $F = \{x = (x_1, \ldots, x_n) \mid \exists u = (u_1 \ldots, u_m), t = (t_1 \ldots, t_m), [g(x, u, t) = 0]\}$.

To define g, we will need an "encoding" function that lets us represent arbitrarily long sequences $(a_1, \ldots, a_N)$ with a pair of numbers (u, t). We will use a technique pioneered by Gödel. Let $\lfloor x/y \rfloor$ denote the floor function, i.e., the greatest integer less than x/y.

Lemma: $z = \lfloor x/y \rfloor$ is a Diophantine relation.

Proof: We present this one example in full to show how a relation that is a reasonable combination of Diophantine relations must itself be Diophantine; other results of this ilk are spread throughout this paper, and the techniques of rigorously proving them will be the same.

First, we note that $z = \lfloor x/y \rfloor \iff yz \leq x < y(z+1)$.

The first of these inequalities can be expressed as follows: $\exists a, [yz + a - x - 1 = 0]$. (Note that the space from which we are choosing variables' values is $\mathbb{Z}^+$.) The second inequality is expressed as $\exists b, [x + b - yz - y = 0]$. To combine these two inequalities, we use the method given earlier for intersecting two r.e. sets, i.e., let $f(x, y, z, a, b) = (yz + a - x - 1)^2 + (x + b - yz - y)^2$. Then $\{(x, y, z) \mid \exists a, b, [f(x, y, z, a, b) = 0]\} = \{(x, y, z) \mid z = \lfloor x/y \rfloor\}$. That is, $z = \lfloor x/y \rfloor$ determines a set which is also the 0-level of a Diophantine polynomial. Thus, it is a Diophantine relation. □

Let "rem(x, y)" denote the remainder function, i.e. the remainder when dividing x by y. $\text{rem}(x, y) = x - y \cdot \lfloor \frac{x}{y} \rfloor$, so rem is also Diophantine. (Briefly, $z = \text{rem}(x, y) \iff (z + y \cdot \lfloor \frac{x}{y} \rfloor - x = 0)$, and by the Diophantine nature of the floor function, the right hand side of the if and only if is a Diophantine polynomial equation.)

Let $\text{gd}(u, k, t) = \text{rem}(1 + kt, u)$. This as well is Diophantine. We want to choose (u, t) such that $\text{gd}(u, k, t) = a_k$ for all $1 \leq k \leq N$. First choose $X \geq N$ such that $\forall k, [1 + kX! > a_k]$, and let $t = X!$. (The lower bound on X and the use of the factorial operation are necessary to ensure that the Chinese remainder theorem will apply below.)

We note that for $k_1 < k_2 \leq N$ we have $\gcd(1 + k_1 t, 1 + k_2 t) = 1$, since any common prime factor would also have to divide $(k_2 - k_1)X!$, but all such primes are $< X$ and thus cannot divide any number of the form $1 + kX!$.

Thus, the Chinese remainder theorem asserts that there is a solution u to the system of equations $u \equiv a_k \pmod{1 + kt}, 1 \leq k \leq N$. u and t serve as our encoding of the sequence of a_k's, and gd extracts the values accordingly.

With that done, let g be defined as follows:

$$g(x_1, \ldots, u_1, \ldots, t_1, \ldots) = \sum_{k=1}^{x_n} [f(x_1, \ldots, x_n, \text{gd}(u_1, k, t_1), \ldots, \text{gd}(u_m, k, t_m))]^2.$$

If there are u_i, t_i such that $f(x_1, \ldots, x_n, \text{gd}(u_1, k, t_1), \ldots, \text{gd}(u_m, k, t_m)) = 0$ for $1 \leq k \leq x_n$, then g will equal 0. But by the definition of bounded universal quantification, we already have the y_{ik}'s that are witnesses to $(x_1, \ldots, x_n)$ being members of E. Thus, we can find the requisite u_i, t_i's that encode the lists $(y_{11}, y_{21}, \ldots, y_{m1}), (y_{12}, y_{22}, \ldots, y_{m2}), \cdots$, and g will indeed equal 0. Note that the finesse of using the gd function was necessary because otherwise, due to the y_{ik}'s, the function g would have had a non-fixed number of arguments.

On the other hand, if g gives a value of 0, then for all $1 \leq k \leq x_n$, we have $(x_1, \ldots, x_{n-1}, k) \in E$. So $(x_1, \ldots, x_n) \in F$.

g is a PRF, having been built up from PRFs f and gd, so {r.e. sets} is closed under bounded

universal quantification. □

Therefore, {D-sets} ⊆ {r.e. sets}. We must still show that {r.e. sets} ⊆ {D-sets}.

By definition, every r.e. set E is the 1-level of some PRF f. One way to look at this is that E is the projection of $[(\mathbb{Z}^+)^n \times 1] \cap \{(x_1, \ldots, x_n, y) \mid f(x_1, \ldots, x_n) = y\}$ to its first n coordinates. The first set of this intersection is clearly a D-set, so if we can show that the second set, i.e., the graph of a PRF f, is a D-set also, then by the closure of D-sets under intersection and projection, every r.e. set E is a D-set.

We do this by considering the definition of primitive recursive functions. First of all, the graphs of all of the basic PRFs were already shown to be Diophantine, so they are D-sets as well.

Now, take two PRFs $f : (\mathbb{Z}^+)^q \to (\mathbb{Z}^+)^r, g : (\mathbb{Z}^+)^p \to (\mathbb{Z}^+)^q$ whose graphs Γ_f, Γ_g are known to be D-sets. $\Gamma_{f \circ g}$ is the projection of $[\Gamma_g \times (\mathbb{Z}^+)^r] \cap [(\mathbb{Z}^+)^p \times \Gamma_f]$ to its first p *and* its last r coordinates. Since D-sets are closed under direct product and intersection, $\Gamma_{f \circ g}$ is a D-set.

Next, take two PRFs $f : (\mathbb{Z}^+)^p \to (\mathbb{Z}^+)^q, g : (\mathbb{Z}^+)^p \to (\mathbb{Z}^+)^r$ whose graphs Γ_f, Γ_g are again known to be D-sets. Let h be the function that comes from juxtaposing f and g. $\Gamma_h = [\Gamma_f \times (\mathbb{Z}^+)^r] \cap \text{perm}_{p,q,r}[\Gamma_g \times (\mathbb{Z}^+)^q]$, where "$\text{perm}_{p,q,r}$" is the operation that switches the places of last q coordinates with the r coordinates before it. (Example: $\text{perm}_{1,2,4}(1,2,2,2,2,3,3) = (1,3,3,2,2,2,2)$. Given any p, q, r, $\text{perm}_{p,q,r}$ can be created from the projection base function using applications of juxtaposition, so it is a PRF.) Since D-sets are closed under direct product and intersection, Γ_h is a D-set.

It remains to show that the operation of recursion preserves the property of being a D-set. We will use the function gd defined earlier; it is Diophantine, so its graph is a D-set. We are given functions $f : (\mathbb{Z}^+)^n \to \mathbb{Z}^+$ and $g : (\mathbb{Z}^+)^{n+2} \to \mathbb{Z}^+$ whose graphs are D-sets, and we want to show that the graph of $h : (\mathbb{Z}^+)^{n+1} \to \mathbb{Z}^+$ is also a D-set, where h behaves as follows:

$$\begin{aligned} h(x_1, \ldots, x_n, 1) &= f(x_1, \ldots, x_n) \\ h(x_1, \ldots, x_n, k+1) &= g(x_1, \ldots, x_n, k, h(x_1, \ldots, x_n, k)) \end{aligned}$$

$\Gamma_h = \{(x_1, \ldots, x_n, y, z) \mid h(x_1, \ldots, x_n, y) = z\}$. Let $\Gamma_1 = \{(x_1, \ldots, x_n, 1, z) \mid (x_1, \ldots, x_n, 1, z) \in \Gamma_h\}$, and let $\Gamma_2 = \Gamma_h - \Gamma_1$, i.e., the part of the graph where h takes values > 1.

$(x_1, \ldots, x_n, y, z) \in \Gamma_1$ if and only if $y = 1$ and $z = f(x_1, \ldots, x_n)$, i.e., $(x_1, \ldots, x_n, z) \in \Gamma_f$. Thus, $\Gamma_1 = \text{perm}_{n,1,1}(\Gamma_f \times \mathbb{Z}^+) \cap \{(x_1, \ldots, x_n, 1, z)\}$. This is clearly a D-set.

As for Γ_2, we consider the following equations (which we will identify with the sets that they determine):

$$\begin{aligned} G_1 &: z = \text{gd}(u, y, t) \\ G_2 &: \text{gd}(u, 1, t) = f(x_1, \ldots, x_n) \\ G_3 &: y > 1 \wedge \forall 2 \leq k \leq y, [\text{gd}(u, k, t) = g(x_1, \ldots, x_n, k-1, \text{gd}(u, k-1, t))] \end{aligned}$$

Taken together, these determine a set G in the $(x_1, \ldots, x_n, y, z, u, t)$ space.

Proposition: $\Gamma_2 \subseteq$ the projection of G to its first $n+2$ coordinates.

Proof: Choose u, t such that they encode the sequence $h(x_1, \ldots, x_n, 1), h(x_1, \ldots, x_n, 2), \cdots, h(x_1, \ldots, x_n, y)$.

G_1 is satisfied, since $(x_1, \ldots, x_n, y, z) \in \Gamma_2$ implies $z = h(x_1, \ldots, x_n, y)$. Then $\text{gd}(u, y, t) = h(x_1, \ldots, x_n, y) = z$.

G_2 is satisfied, since $\text{gd}(u, 1, t) = h(x_1, \ldots, x_n, 1) = f(x_1, \ldots, x_n)$.

$(x_1, \ldots, x_n, y, z) \in \Gamma_2$ also implies $y > 1$. Thus, we can show by induction on k that G_3 holds: G_2 provides the base case, and the inductive step holds trivially from the comparison of the G_3 condition to the definition of primitive recursion. $\square$

Proposition: (The projection of G to its first $n+2$ coordinates) $\subseteq \Gamma_2$.

Proof: Take any $(x_1, \ldots, x_n, y, z, u, t) \in G$. Then, by G_2 and G_3, u, t encode the following sequence $\{a_1, a_2, \ldots, \}$:

$$\begin{aligned}
a_1 &= f(x_1, \ldots, x_n) = h(x_1, \ldots, x_n, 1), \\
a_2 &= g(x_1, \ldots, x_n, 1, f(x_1, \ldots, x_n)) = h(x_1, \ldots, x_n, 2), \\
a_3 &= g(x_1, \ldots, x_n, 2, h(x_1, \ldots, x_n, 2)) = h(x_1, \ldots, x_n, 3), \\
&\vdots \\
a_y &= g(x_1, \ldots, x_n, y, h(x_1, \ldots, x_n, y-1)) = h(x_1, \ldots, x_n, y).
\end{aligned}$$

By G_1, $z = \text{gd}(u, y, t) = a_y = h(x_1, \ldots, x_n, y)$, and by G_3, $y > 1$, so $(x_1, \ldots, x_n, y, z) \in \Gamma_2$. $\square$

Therefore, $\Gamma_2 =$ the projection of G to its first $n+2$ coordinates. It remains to show that each of G_1, G_2, G_3 determines D-sets; then by the closure of D-sets under intersection and projection, Γ_2 will be a D-set.

G_1 is simply the graph of the gd function, with extra coordinates $x_1, \ldots, x_n$. From the definition of gd, the set determined by G_1 can be expressed as a projection of $\{(x_1, \ldots, x_n, y, z, u, t, w) \mid \text{rem}(1 + yt, u) - w = 0\}$. We have already shown rem to be Diophantine, so G_1 is a D-set.

G_2 is the a projection of the intersection of the following D-sets: $k - 1 = 0, w = \text{gd}(u, k, t)$, $f(x_1, \ldots, x_n) - w = 0$, where we have introduced auxiliary variables k, w. Thus, G_2 is a D-set.

For G_3, consider the following equations:

$$\begin{aligned}
z &= \text{gd}(u, y', t) \\
w &= \text{gd}(u, y' + 1, t) \\
w &= g(x_1, \ldots, x_n, y', z)
\end{aligned}$$

Each of the sets determined by equations is a D-set, so taken together, they define a D-set; call it F. Applying the bounded universal quantifier to the y' coordinate of F then gives us a set F' defined as follows: $(x_1, \ldots, x_n, y', z, u, t) \in F' \iff \forall 1 \leq k \leq y', [\text{gd}(u, k+1, t) = g(x_1, \ldots, x_n, k, \text{gd}(u, k, t))]$.

On the other hand, $(x_1, \ldots, x_n, y, z, u, t) \in G_3 \iff \forall 1 \leq k \leq y - 1, [\text{gd}(u, k+1, t) = g(x_1, \ldots, x_n, k, \text{gd}(u, k, t))]$. Thus, $G_3 =$ projection of $\{(x_1, \ldots, x_n, y, z, u, t, y') \mid y' - (y-1) = 0 \wedge (x_1, \ldots, x_n, y', z, u, t) \in F'\}$ to its first $n+4$ coordinates. F' is a D-set, so G_3 is a D-set.

Combining all of the above results, we finally conclude that {r.e. sets} = {D-sets}.

3 The reduction to exponentiation

The proof that {r.e. sets} = {D-sets} was relatively long but mostly for technical reasons. Showing that {Diophantine sets} = {D-sets} is a much more difficult proposition. From the definition, we have {Diophantine sets} $\subseteq$ {D-sets}. The result {D-sets} $\subseteq$ {Diophantine sets} was historically the last step completed in the overall proof. The goal of this section is to show why the Diophantine nature of exponentiation is important to this step. Thus, for the remainder of this section, we

will assume that exponentiation is a Diophantine relation; we will turn to the actual proof of exponentiation's Diophantine nature in the next section.

First, we show that the graphs of some other "elementary" functions are Diophantine.

Lemma: If $u > n^k$ and $n \geq k$, then $\binom{n}{k} = \text{rem}(\lfloor (u+1)^n / u^k \rfloor, u)$.

Proof:

$$\frac{(u+1)^n}{u^k} = \sum_{i=0}^{k-1} \binom{n}{i} u^{i-k} + \binom{n}{k} + \sum_{i=k+1}^{n} \binom{n}{i} u^{i-k}$$

By simple estimation, $\binom{n}{i} \leq n^i$, so $\sum_{i=0}^{k-1} \binom{n}{i} u^{i-k} \leq \frac{n^0}{u^k} + \frac{n^1}{u^{k-1}} + \cdots + \frac{n^{k-1}}{u^1}$. $u > n^k$, so this expression in turn $< \frac{1}{n^{k \cdot k}} + \frac{n}{n^{k(k-1)}} + \cdots + \frac{n^{k-1}}{n^k} < k \cdot \frac{1}{n} \leq 1$. Thus, the floor operation eliminates the first term. The last term is divisible by u. The middle term, $\binom{n}{k}$, is less than u, since $u > n^k \geq \binom{n}{k}$. The lemma follows. □

We know that $z = \lfloor x/y \rfloor$ and $z = \text{rem}(x, y)$ are Diophantine relations, and if exponentiation is also assumed to be Diophantine, this lemma proves that $\binom{n}{k}$ is a Diophantine relation. With that in hand, we can show the factorial relation is Diophantine as well:

Lemma: For $k > 0$ and $n > (2k)^{k+1}$, $k! = \lfloor n^k / \binom{n}{k} \rfloor$.

Proof: First,

$$\frac{n^k}{\binom{n}{k}} = \frac{n^k k!}{n(n-1)\cdots(n-k+1)} = k! \cdot \frac{1}{(1-1/n)\cdots(1-(k-1)/n)} > k!.$$

$k/n < \frac{1}{2}$, so:

$$1 + \frac{2k}{n} = 1 + \frac{k}{n}\left(1 + \frac{1}{2} + \frac{1}{4} + \cdots\right) > 1 + \frac{k}{n}\left(1 + \frac{k}{n} + \left(\frac{k}{n}\right)^2 + \cdots\right) = \frac{1}{1 - k/n}.$$

Furthermore,

$$\left(1 + \frac{2k}{n}\right)^k = \sum_{j=0}^{k} \binom{k}{j} \binom{2k}{n}^j < 1 + \frac{2k}{n} \sum_{j=1}^{k} \binom{k}{j} < 1 + \frac{2k}{n} \cdot 2^k.$$

Thus,

$$\frac{n^k}{\binom{n}{k}} = k! \cdot \frac{1}{(1-1/n)\cdots(1-(k-1)/n)} < k! \cdot \frac{1}{(1-k/n)^k}$$
$$< k! \cdot \left(1 + \frac{2k}{n}\right)^k < k! + k! \cdot \frac{2k}{n} \cdot 2^k < k! + \frac{2^{k+1} k^{k+1}}{n} < k! + 1$$

Therefore, $k! < \frac{n^k}{\binom{n}{k}} < k! + 1$, and the lemma follows. □

We note that, without any further work, we can now deduce that the set of primes is Diophantine. That is, a is prime $\iff [a > 1 \wedge \gcd(a, (a-1)!) = 1]$, and we can now express the right-hand side of the if and only if as a system of Diophantine equations which may be combined into a single Diophantine equation by the technique elaborated upon earlier. Written out explicitly, this would

be a very complex expression; later we will see a more compact Diophantine equation for the set of primes.

We now show that a pair of somewhat more complicated functions that we will need shortly are Diophantine:

Lemma: $z = \prod_{1 \le j \le Y}(Y_1 - j) \wedge Y_1 > Y$ is Diophantine.

Proof: By pure algebraic manipulation, $z = \prod_{1 \le j \le Y}(Y_1 - j) \wedge Y_1 > Y$ is equivalent to $z = Y!\binom{Y_1}{Y} \wedge Y_1 > Y$. This is Diophantine. □

Lemma: $z = \prod_{1 \le k \le y}(1 + kn)$ is Diophantine.

Proof: We introduce additional variables u, v which will later be projected out. Let $u = n(1 + yn)^y + 1$; note that this is a Diophantine relation. $\gcd(u, n) = 1$ and $u > \prod_{1 \le k \le y}(1 + kn)$, so $\exists v, [vn \equiv 1 (\mathrm{mod}\ u)]]$.

Consider $n^y y!\binom{v+y}{y} = n^y(v+y)(v+y-1)\cdots(v+1) = (vn+yn)(vn+(y-1)n)\cdots(vn+n)$. Taken mod u, this last expression is congruent to $(1+yn)(1+(y-1)n)\cdots(1+n) = \prod_{1 \le k \le y}(1+kn)$. In fact, since $u > \prod_{1 \le k \le y}(1+kn)$, we have that $\prod_{1 \le k \le y}(1+kn) = \mathrm{rem}(n^y y!\binom{v+y}{y}, u)$. The right-hand side of this equation is Diophantine, and the lemma is proven. □

We finally turn back to D-sets. Since the Diophantine sets are closed under finite union, finite intersection, finite direct product, and projection (the proof is the same as that given for the closure properties of the r.e. sets), we need only show that applying the bounded universal quantifier to a Diophantine set yields another Diophantine set.

We begin with a Diophantine set E, represented as the projection of the 0-level set of some Diophantine polynomial $f(x_1, \ldots, x_n, k, y_1, \ldots, y_m)$ onto its first $n+1$ coordinates (using $n+1$ will simplify later expressions). Let D be the set obtained from bounded universal quantification on the $(n+1)$th coordinate of E, i.e.,$(x_1, \ldots, x_n, z) \in D \iff$ for $1 \le k \le z$, there are $y_{1k}, \ldots, y_{mk}$ such that $f(x_1, \ldots, x_n, k, y_{1k}, \ldots y_{mk}) = 0$. Also, let c be the sum of the absolute values of the coefficients of f, and let d be f's degree.

Now consider the following set of equations (the last one is actually shorthand for m separate equations):

$$\begin{aligned}
1 + KN! &= \prod_{k=1}^{z}(1 + kN!) \\
N &\ge c(x_1 \cdots x_n z Y)^d \wedge Y < Y_1 \wedge \cdots \wedge Y < Y_m \\
f(x_1, \ldots, x_n, K, Y_1, \ldots, Y_m) &\equiv 0 \ (\mathrm{mod}\ 1 + KN!) \\
\prod_{j \le Y}(Y_i - j) &\equiv 0 \ (\mathrm{mod}\ 1 + KN!) \qquad (i = 1, \ldots, m)
\end{aligned}$$

By the results worked out earlier in this section, these equations determine a Diophantine set D' in the $(x_1, \ldots, x_n, z, Y, N, K, Y_1, \ldots, Y_m)$ space.

Proposition: $D \subseteq$ the projection of D' to its first $n+1$ coordinates.

Proof: It suffices, given $(x_1, \ldots, x_n, z) \in D$, to find values for the other coordinates, i.e., $K, Y, N, Y_1, \ldots, Y_m$, such that the equations defining D' are satisfied.

K is determined by the first equation.

Since D is a D-set, for $1 \le k \le z$, there are $y_{1k}, \ldots, y_{mk}$ such that $f(x_1, \ldots, x_n, k, y_{1k}, \ldots y_{mk}) = 0$.

Let $Y = \max[z \cup \bigcup_{i \leq m, k \leq z} y_{ik}]$.

Recall the gd function; we will now use it to encode the y_{ik}'s into the Y_i's (and $N!$). That is, we solve:

$$\mathrm{gd}(Y_i, k, N!) = y_{ik}$$

for all $1 \leq i \leq m, 1 \leq k \leq z$. This is possible by the previously proved properties of gd. Furthermore, we may choose N arbitrarily large, so the Y_i's can be made arbitrarily large as well (specifically, by repeatedly adding $1 + kN!$). In particular, both N and the Y_i's can be made large enough such that they satisfy the second equation/inequality.

By the definition of gd, $1 + kN! \mid Y_i - y_{ik}$. We know that any $y_{ik} \leq Y < Y_i$, so for all i, $1 + kN! \mid \prod_{j \leq Y}(Y_i - j)$. Also, for any $k_1 < k_2 \leq z$, $\gcd(1 + k_1 N!, 1 + k_2 N!) = 1$. (Proof: Any common factor p would have to also divide $(k_2 - k_1)N!$. By the second equation/inequality $z \leq N$, so $p \mid N$. But no such p can divide $1 + k_1 N!$.) By the first equation, $1 + KN! \mid \prod_{j \leq Y}(Y_i - j)$, and the last set of equations is satisfied.

Also by the first equation, $(1 + KN!) - (1 + kN!) \equiv 0 \pmod{1 + kN!}$, so $K \equiv k \pmod{1 + kN!}$. By the way we chose the Y_i's, $Y_i \equiv y_{ik} \pmod{1 + kN!}$. Thus, since f is a Diophantine polynomial, $f(x_1, \ldots, x_n, K, Y_1, \ldots, Y_m) \equiv f(x_1, \ldots, x_n, k, y_{ik}, \ldots, y_{mk}) \equiv 0 \pmod{1 + kN!}$. This directly implies the third equation, and the proposition is proved. $\square$

Proposition: The projection of D' to its first $n + 1$ coordinates $\subseteq D$.

Proof: It suffices, given $(x_1, \ldots, x_n, z, Y, N, K, Y_1, \ldots, Y_m) \in D'$, to find values for y_{ik} $(1 \leq i \leq m, 1 \leq k \leq z)$ such that $f(x_1, \ldots, x_n, k, y_{1k}, \ldots, y_{mk}) = 0$. First, we let p_k be any prime such that $p_k \mid 1 + kN!$. Note that from this, all the p_k's must be $> N$.

Also, $p_k \mid 1 + KN! \mid \prod_{j \leq Y}(Y_i - j)$. p_k is prime, so there is some $j \leq Y$ such that $p_k \mid Y_i - j$. Let $y_{ik} = j$; in other words, $y_{ik} = \mathrm{rem}(Y_i, p_k)$.

All the y_{ik}'s are thus $\leq Y$, so $f(x_1, \ldots, x_n, k, y_{1k}, \ldots, y_{mk}) \leq c(x_1 \cdots x_n z Y)^d$ (since f is a polynomial). By the second equation/inequality, $f(x_1, \ldots, x_n, k, y_{1k}, \ldots, y_{mk}) \leq N < p_k$.

Meanwhile, we know $f(x_1, \ldots, x_n, K, Y_1, \ldots, Y_m) \equiv 0 \pmod{1 + KN!}$ and $K \equiv k \pmod{1 + kN!}$, so:

$$f(x_1, \ldots, x_n, k, y_{1k}, \ldots, y_{mk}) \equiv f(x_1, \ldots, x_n, K, Y_1, \ldots, Y_m) \equiv 0 \pmod{p_k}.$$

Therefore, $f(x_1, \ldots, x_n, k, y_{1k}, \ldots, y_{mk})$ must $= 0$ for all k $(1 \leq k \leq z)$. Thus, we have found appropriate y_{ik}'s that are witnesses to the fact that $(x_1, \ldots, x_n, z) \in D$. $\square$

Combining all the above results, {r.e. sets} = {D-sets} = {Diophantine sets}.

4 The Diophantine nature of exponentiation

To derive the results of the previous section, we had to assume that exponentiation was a Diophantine relation, a fact that turns out to be far from obvious (cf. Tarski, who conjectured that exponentiation was *not* Diophantine). As stated in the introduction, it was Matiyasevich who provided this last piece of the puzzle in 1970. Manin's version of the proof follows Davis' approach of abandoning Fibonacci numbers in favor of examining another concept familiar to number theorists: Pell's equation, i.e., $x^2 - dy^2 = 1$. In particular, we will look at the solutions to the equation:

$$x^2 - (a^2 - 1)y^2 = 1$$

(We disregard the trivial solution $(1, 0)$.) The theory on Pell's equations gives us the result that if (x_1, y_1) is the solution with the least first coordinate, then any other solution (x_i, y_i) can be determined from the equation $x_i + y_i\sqrt{d} = (x_1 + y_1\sqrt{d})^i$ (in this case, we have $d = a^2 - 1$)

We create functions $x_n(a), y_n(a)$ which denote the coordinates of nth solutions of $x^2 - (a^2 - 1)y^2 = 1$. Conveniently, for this special Pell's equation, the first solution will always be the trivial $(a, 1)$, so $x_1(a) = a$ and $y_1(a) = 1$. Furthermore, since $x_{i+1}(a) + y_{i+1}(a)\sqrt{a^2-1} = (x_1(a) + y_1(a)\sqrt{a^2-1})(x_i(a) + y_i(a)\sqrt{a^2-1})$, we have the recurrence relations:

$$\begin{aligned} x_{i+1}(a) &= ax_i(a) + (a^2 - 1)y_i(a) \\ y_{i+1}(a) &= x_i(a) + ay_i(a) \end{aligned}$$

These will be useful later. One particularly important consequence of them is that $x_i(a), y_i(a)$ are both strictly increasing functions.

We will prove that $y_n(a)$ is a Diophantine function, but first let us see why that result will lead to a proof that exponentiation is Diophantine:

Lemma: $z = y_n(a)$ is Diophantine $\implies$ $m = a^n$ is Diophantine

Proof: Clearly, if $a = 1$, $m = a^n$ is Diophantine, so we assume for the rest of the proof that $a > 1$.

We first show that $(2a - 1)^n \leq y_{n+1}(a) \leq (2a)^n$, by induction. A quick calculation shows that $y_2(a) = 2a$, so the base case checks: $2a - 1 \leq 2a \leq 2a$. By manipulation of the recurrence relation for $y_n(a)$, we find that $y_{n+2}(a) = ay_{n+1}(a) + x_{n+1}(a) = \left(a + \frac{x_{n+1}(a)}{y_{n+1}(a)}\right) \cdot y_{n+1}(a)$. By Pell's equation itself, we have:

$$\frac{x_{n+1}(a)}{y_{n+1}(a)} = \sqrt{a^2 - 1 + \frac{1}{y_{n+1}(a)^2}} < a$$

Furthermore, $a - 1 < \sqrt{a^2 - 1 + \frac{1}{y_{n+1}(a)^2}}$. Thus, $(2a - 1) \cdot y_{n+1}(a) < y_{n+2}(a) < 2a \cdot y_{n+1}(a)$. Thus, by induction, $(2a - 1)^n \leq y_{n+1}(a) \leq (2a)^n$.

Thus,

$$a^n \left(1 - \frac{1}{2Na}\right)^n = \frac{(2Na - 1)^n}{(2N)^n} \leq \frac{y_{n+1}(Na)}{y_{n+1}(N)} \leq \frac{(2Na)^n}{(2N - 1)^n} = a^n \frac{1}{(1 - \frac{1}{2N})^n}$$

If we choose N "large enough", it will ensure that the closest integer to $y_{n+1}(Na)/y_{n+1}(N)$ will be a^n. "Closest integer" can be defined in a Diophantine fashion, so the problem thus becomes how to define "large enough" in a Diophantine fashion. By simple binomial expansion, we know that

$$\left(1 - \frac{1}{2Na}\right)^n \geq 1 - \frac{n}{2Na}.$$

Similarly,

$$\frac{1}{(1 - \frac{1}{2N})^n} \leq \frac{1}{1 - \frac{n}{2N}} = \left(1 - \frac{n}{2N}\right)^{-1} \leq 1 + \frac{n}{N}.$$

Thus, we have:

$$a^n\left(1-\frac{n}{2Na}\right) \le \frac{y_{n+1}(Na)}{y_{n+1}(N)} \le a^n\left(1+\frac{n}{N}\right)$$
$$a^n - \frac{a^n\cdot n}{2Na} \le \frac{y_{n+1}(Na)}{y_{n+1}(N)} \le a^n + \frac{a^n\cdot n}{N}.$$

So, if we choose $N > 2na^n$, then $a^n - \frac{1}{2} < \frac{y_{n+1}(Na)}{y_{n+1}(N)} < a^n + \frac{1}{2}$. But $a^n \le (2a-1)^n \le y_{n+1}(a)$, so it suffices to take $N > 2n\cdot y_{n+1}(a)$, and this last inequality is a Diophantine relation. The lemma is proved. □

All that now remains is to prove that $y = y_n(a)$ is a Diophantine relation. This was by no means an obvious development: Julia Robinson had already anticipated the possibility of using Pell's equation in this vein in [Robinson], but it would be nearly twenty years before anyone actually did so (see [Davis1973]), and even then it was only inspired by the techniques that Matiyasevich used for his own proof.

For maximum ease of understanding, we will use the convention that variable names from late in the alphabet will denote solutions to (some) Pell's equation, and variable names from early in the alphabet will denote numbers that are related to the free coefficient in Pell's equation (d in our initial presentation).

We first note that by induction on n and the use of the recurrence relations for $x_n(a), y_n(a)$, it is simple to show that:

$$\begin{aligned} x_n(a) &= a^n + \sum_{i=1}^{\lfloor n/2\rfloor}\binom{n}{2i}a^{n-2i}(a^2-1)^i \\ y_n(a) &= \sum_{i=1}^{\lfloor (n+1)/2\rfloor}\binom{n}{2i-1}a^{n-2i+1}(a^2-1)^{i-1} \end{aligned}$$

Now consider the following set of equations:

$$\begin{aligned} D_1 &: y \ge n \wedge a > 1 \\ D_2 &: x^2 - (a^2-1)y^2 = 1 \\ D_3 &: v \equiv 0 \pmod{4y^2} \\ D_4 &: u^2 - (a^2-1)v^2 = 1 \\ D_5 &: b = a + u^2(u^2-a) \\ D_6 &: s^2 - (b^2-1)t^2 = 1 \\ D_7 &: s \equiv x \pmod{u} \\ D_8 &: t \equiv n \pmod{4y} \end{aligned}$$

Taken together, these clearly define a Diophantine set; call it D.

How are we to grasp the meaning of these equations intuitively? Note that, taken mod $a-1$, all the terms of the sum for $y_n(a)$ drop out except the first one; thus, $y_n(a) \equiv n \pmod{a-1}$. Thus, the Diophantine equation $x^2 - (a^2-1)y^2 = 1 \wedge y \equiv n \pmod{a-1}$ suffices to determine the set $\{(y,n,a,x) \mid \exists z, [y = y_{n+z(a-1)}(a)]\}$. Equations $D_3 - D_8$ basically serve to pare down this set to only the case where $z = 0$, i.e., $y = y_n(a)$, but showing that this is the case requires many details from the properties of solutions of Pell's equation. We will do this below.

That is, let E be the set determined by the relation $y = y_n(a)$. We will show that $E =$ the projection of D to the coordinates (y, n, a).

Proposition: $E \subseteq$ the projection of D to the coordinates (y, n, a).

Proof: Given $y = y_n(a)$, we must find values for x, u, v, s, t, b such that $D_1 - D_8$ are satisfied.

Certainly we have that $y \geq n$ and $a > 1$, since $y_n(a) \geq n$ (proved by induction). Thus, D_1 is already satisfied. x is uniquely determined from D_2, which will thus be satisfied.

Take $(u, v/4y^2)$ to be any solution of the equation $X^2 - (a^2 - 1)(4y^2)^2Y^2 = 1$ (the theory of Pell's equations guarantees that there is a solution, since $(a^2-1)(4y^2)^2$ cannot be a perfect square). This will satisfy both D_3 and D_4. With u chosen, b is uniquely determined by D_5.

Take s, t to be the nth solutions for D_6, i.e., $s = x_n(b), t = y_n(b)$. This completes the choices; we must still show that D_7 and D_8 are satisfied.

We can discern from the sum expression for $x_n(a)$ that $(x_n(j) - x_n(k)) \equiv 0 \pmod{j-k}$, since $j - k \mid j^l - k^l$ for any $l > 0$. Thus, $(x_n(b) - x_n(a)) \equiv 0 \pmod{u^2(u^2 - a)}$, which implies $s - x \equiv 0 \pmod{u}$, so D_7 is satisfied.

Now, $4y \mid 4y^2$, so by D_3, $4y \mid v$. Substituting D_4 into D_5, we have $b = a + (1 + (a^2 - 1)v^2)(1 + (a^2 - 1)v^2 - a)$, and taking this mod $4y$ yields $b - 1 \equiv 0 \pmod{4y}$. As for $x_n(a)$, we can discern from the sum expression for $y_n(a)$ that $(y_n(j) - y_n(k)) \equiv 0 \pmod{j-k}$. Thus, we know that $(y_n(b) - y_n(1)) \equiv 0 \pmod{b-1}$.

What is $y_n(1)$? By the sum expression, $y_n(1) = n$. (This may strike one as a little bit odd, but the expressions also give us that $x_n(1) = 1$, and certainly, $1^2 - 0 \cdot n^2 = 1$.) Thus, $t \equiv n \pmod{4y}$, and D_8 is satisfied. $\square$

Proposition: (The projection of D to the coordinates $(y, n, a)) \subseteq E$.

Proof: This direction is quite a bit more complicated than the other one. We are given $y, n, a, x, u, v, s, t, b$ satisfying $D_1 - D_8$, and we want to show that y is the second coordinate of the nth solution of $x^2 - (a^2 - 1)y^2 = 1$.

Since D_2 is satisfied, we do not have to worry about (x, y) being *some* solution of $x^2-(a^2-1)y^2 = 1$. Thus, by the theory of Pell's equations, (x, y) is the Nth solution of said equation for some N; similarly, let N' be the number such that (u, v) is the N'th solution, and let N_b be the number such that (s, t) is the N_bth solution of $x^2 - (b^2 - 1)y^2 = 1$. We need only show that N must $= n$.

As was shown in the proof of the other direction, D_4 and D_5 give us that $4y \mid b - 1$. Also, $(y_{N_b}(b) - y_{N_b}(1)) \equiv 0 \pmod{b-1}$, so $t \equiv N_b \pmod{4y}$. Combining this with D_8 gives us that $N_b \equiv n \pmod{4y}$. The rest of the proof of this direction is simply to find a particular constraint on N and N_b that, when combined with this result, gives us $n = N$.

$x_{i+j}(a)+y_{i+j}(a)\sqrt{a^2-1} = (x_i(a)+y_i(a)\sqrt{a^2-1})(x_j(a)+y_j(a)\sqrt{a^2-1})$, so $y_{i+j}(a) = y_j(a)x_i(a)+y_i(a)x_j(a)$. Induction then tells us that $y_i(a) \mid y_{ij}(a)$. We also note that since $1/(x_j(a) + y_j(a)\sqrt{a^2-1}) = x_j(a) - y_j(a)\sqrt{a^2-1}$, we have $y_{i-j}(a) = y_i(a)x_j(a) - y_i(a)x_j(a)$.

Suppose $N \not| N'$, i.e. $N' = qN + r$ for some $0 < r < N$. Thus,

$$y_{N'}(a) = y_r(a)x_{qN}(a) + y_{qN}(a)x_r(a).$$

By D_3, $y^2 \mid v$, i.e., $(y_N(a))^2 \mid y_{N'}(a)$. Thus, $y_N(a) \mid y_{N'}(a)$. Also, $y_N(a) \mid y_{qN}(a)$, so $y_N(a) \mid y_r(a)x_{qN}(a)$. But $x_{qN}(a)$ and $y_{qN}(a)$, being a solution of a Pell's equation, cannot share a common factor (such a factor would have to divide into 1); thus, $y_N(a) \not| x_{qN}(a)$. Therefore, $y_N(a) \mid y_r(a)$. But $r < N$, and $y_i(a)$ increases with i. This is a contradiction, so $N \mid N'$; let k be such that $N' = kN$.

Further examination of $x_{kN}(a)+y_{kN}(a)\sqrt{a^2-1} = (x_N(a)+y_N(a)\sqrt{a^2-1})^k$ yields, by binomial

expansion:

$$v = \sum_{i \le k, i \equiv 1 (\mathrm{mod}\ 2)} \binom{k}{i} x^{k-i} y^i (a^2-1)^{(i-1)/2}.$$

mod y^3, everything but the first term drops out, leaving $v \equiv kx^{k-1}y \pmod{y^3}$. Since $y^2 \mid v$ and $y^2 \mid y^3$, we have that $y^2 \mid kx^{k-1}y$, i.e., $y \mid kx^{k-1}$. But, as before, x and y can share no common factors, so $y \mid k$. By the definition of k, $y \mid N'$.

Now,

$$\begin{aligned}
x_{2N' \pm N_b}(a) &= x_{N'}(a)x_{N' \pm N_b}(a) + (a^2-1) \cdot y_{N'}(a)y_{N' \pm N_b}(a) \\
&\equiv (a^2-1)y_{N'}(a)y_{N' \pm N_b}(a) \pmod{x_{N'}(a)} \\
&\equiv (a^2-1)y_{N'}(a)[y_{N'}(a)x_{N_b}(a) \pm y_{N_b}(a)x_{N'}(a)] \pmod{x_{N'}(a)} \\
&\equiv (a^2-1)(y_{N'}(a))^2 x_{N_b}(a) \pmod{x_{N'}(a)} \\
&\equiv [(x_{N'}(a))^2 - 1]x_{N_b}(a) \pmod{x_{N'}(a)} \\
&\equiv -x_{N_b}(a) \pmod{x_{N'}(a)}
\end{aligned}$$

From this, we further conclude that $x_{4N' \pm N_b}(a) \equiv -x_{2N' \pm N_b}(a) \equiv x_{N_b}(a) \pmod{x_{N'}(a)}$. This means that $x_i(a) \pmod{x_{N'}(a)}$ has a period of $4N'$ with respect to the subscript i. The first N' values, mod $x_{N'}(a)$, are congruent to $x_0(a), x_1(a), \cdots, x_{N'-1}(a)$. Then $x_{N'}(a), x_{N'+1}(a), \cdots, x_{2N'-1}(a)$ are congruent to $0, -x_{N'-1}(a), -x_{N'-2}(a), \cdots, -x_1(a), -x_0(a)$, and $x_{2N'}(a), \cdots, x_{4N'-1}(a)$ are congruent to $0, x_{2N'-1}(a), x_{2N'-2}(a), \cdots, x_1(a)$ (all mod $x_{N'}(a)$). Thus, with the subscript of $x_i(a)$ ranging from 0 to $4N'-1$, the sequence looks like this:

$$x_0, x_1, \cdots, x_{N'-1}, 0, -x_{N'-1}, -x_{N'-2}, \cdots, -x_1, -x_0, -x_1, \cdots, -x_{N'-1}, 0, x_{N'-1}, \cdots, x_1$$

("(a)"'s omitted for brevity.) Since $x_i(a)$ increases with i, $x_0(a), x_1(a), \cdots, x_{N'-1}(a)$ actually *are* the remainders one gets when dividing $x_0(a), x_1(a), \cdots, x_{N'-1}(a)$ into $x_{N'}(a)$. Thus, the first N' remainders are all unique (otherwise, $x_i(a) = x_j(a)$ for $i < j < N'$, a clear impossibility).

Now, D_5 implies that $u \mid b-a$. Since $(x_{N_b}(b) - x_{N_b}(a)) \equiv 0 \pmod{b-a}$, we have that $x_{N_b}(b) \equiv x_{N_b}(a) \pmod{u}$. Combining with D_7, $x_N(a) \equiv x_{N_b}(a) \pmod{x_{N'}(a)}$. We split briefly into two cases:

Case 1: $x_{N'}(a)$ is odd.

By the recurrence relation for $x_i(a)$, we know that for $i < N'$, $x_i(a) \le x_{N'}(a)/a \le \frac{1}{2}x_{N'}(a)$. Thus, all of $0, -x_{N'-1}, -x_{N'-2}, \cdots, -x_0$, i.e., $x_{N'}(a)$ through $x_{2N'}(a)$, are distinct from $x_0(a), x_1(a), \cdots, x_{N'-1}(a)$ as well as from each other. Therefore, $x_0(a), x_1(a), \cdots, x_{2N'}(a)$ form a mutually unique set of residues mod $x_{N'}(a)$.

Assume that $x_i(a) \equiv x_{N_b}(a) \pmod{x_{N'}(a)}$. $N \mid N'$ and $N \neq N'$, so $N < N'$. This means that if $0 \le i \le 2N'$, then $i = N$, by the result of the previous paragraph. If $2N' < i < 4N'$, then since $x_{4N'-i}(a) \equiv -x_{2N'-i}(a) \equiv x_i(a) \pmod{x_{N'}(a)}$ (same argument as given above concerning $x_{2N' \pm N_b}(a)$), $i = 4N' - N$. The periodicity of $x_i(a) \pmod{x_{N'}(a)}$ then guarantees the following:

$$x_i(a) \equiv x_N(a) \pmod{x_{N'}(a)} \implies i \equiv \pm N \pmod{4N'}.$$

In particular, $N_b \equiv \pm N \pmod{4N'}$.

Case 2: $x_{N'}(a)$ is even.

We would like to show the same result as Case 1, but there is a minor complication. As in Case 1, for $i < N'$, $x_i(a) \leq x_{N'}(a)/a \leq \frac{1}{2}x_{N'}(a)$. Everything, in fact, will work as in Case 1 except for the case when $x_{N'-1}(a) = \frac{1}{2}x_{N'}(a)$.

If this is the case, then $x_{N'+1}(a) \equiv -\frac{1}{2}x_{N'}(a) \equiv \frac{1}{2}x_{N'}(a) \equiv x_{N'-1}(a) \pmod{x_{N'}(a)}$, which would contradict our sought-for result (that is, $x_i(a) \equiv x_N(a) \pmod{x_{N'}(a)} \implies i \equiv \pm N \pmod{4N'}$). However, $N < N'$, so since N also divides N', N cannot equal $N' - 1$, except in the even more special case that $N = 1, N' = 2$. But this case is impossible under these circumstances: $x_{N'}(a) = x_2(a) = ax_1(a) + (a^2 - 1)y_1(a) = 2a^2 - 1$ is not an even number.

Thus, everything really does work as in Case 1, and $N_b \equiv \pm N \pmod{4N'}$.

$y \mid N'$, so $N_b \equiv \pm N \pmod{4y}$. This is the condition on N and N_b that was mentioned at the beginning of the proof of this direction. Combining it with $N_b \equiv n \pmod{4y}$ gives us $n \equiv \pm N \pmod{4y}$.

Now $n \leq y$ (by D_1) and $N \leq y$ (because $N \leq y_N(a)$), and n and N are both positive integers, so $n + N \leq 2y$ and $|n - N| < y$.

If $n \equiv -N \pmod{4y}$, then $\exists Z \in \mathbb{Z}, [n - 4yZ = -N]$. Then $n + N = 4yZ$, which, taken with $n + N \leq 2y$, implies $Z = 0$ and $n = -N$. But this is clearly impossible, as n and N are both positive integers. Thus, $n \equiv N \pmod{4y}$, and $\exists Z' \in \mathbb{Z}, [n - 4yZ' = N]$. Then $n - N = 4yZ'$, which with $|n - N| < y$ implies $Z' = 0$ and $n = N$. $\square$

$y_n(a)$ is Diophantine, and hence, exponentiation is Diophantine also.

5 A compact prime-defining polynomial

The insolubility of Hilbert's tenth problem is the most celebrated of the consequences of the work of Robinson, Davis, Putnam, and Matiyasevich. There are many other negative consequences that fall out of the result, including the seemingly paradoxical fact that, for any specific axiomatization of mathematics, there is a Diophantine equation possessing two properties: it has no solution in the positive integers, and this unsolvability is unprovable in the axiomatization. (This is, of course, an extension of Gödel's incompleteness results.)

However, there are also positive consequences. One of the most interesting of these is the existence of a single polynomial whose positive values are precisely the prime numbers when its variables range over $\mathbb{N}$ (this is, of course, just as easily done over $\mathbb{Z}^+$, as we have done in this paper thus far, but allowing 0 does make for simpler expressions in this case). This fact rises immediately out of the Diophantine nature of the set of prime numbers, as well as the simple observation that if a set $\subset \mathbb{N}$ can be defined as the projection of the 0-level of a Diophantine polynomial f onto one of its coordinates, say, x_1, then said set is also equal to the set of positive values of the polynomial $x_1[1-(f(x_1, \ldots, x_n))^2]$. However, trying to construct such a polynomial from the methods presented in this paper would result in an expression that was, to say the least, unwieldy. Using specialized techniques can streamline the expression. The most compact known polynomial with the desired property is derived in [Jones].

The polynomial depends on Wilson's theorem, which states that $k+1$ is prime iff $k+1 \mid k! + 1$. Thus, a compact Diophantine definition of factorial is required. We begin by eliminating variables from equations $D_1 - D_8$ of section 4:

Proposition: The set defined by the relation $y = y_n(a)$ (where $n \geq 1$ and $a \geq 2$) is a projection

of the set defined by

$$\begin{aligned} x^2 - (a^2-1)y^2 &= 1 \\ u^2 - 16(a^2-1)r^2y^4 &= 1 \\ (x+cu)^2 - ((a+u^2(u^2-a))^2-1)(n+4dy)^2 &= 1 \\ n &\leq y \end{aligned}$$

(Note that variables c, d, r have been introduced; these come from the congruences E_7, E_8, E_3.)

We will need the following result, which will be referred to as the "exponential growth" lemma:

Lemma: For $e \geq 1$, $e^3(e+2)(n+1)^2+1 = \alpha^2$ implies that $e-1+e^{e-2} \leq n$. Also, for any β, there is an n such that $\beta \mid n+1$ and the given equation is still satisfied.

Proof: Assume n solves the equation. By some algebra, we have $\alpha^2-(e+1-1)^3(e+1+1)(n+1)^2 = 1$, or $\alpha^2 - ((e+1)^2-1)[e(n+1)]^2 = 1$. This is a Pell's equation; thus, there is some j such that $y_j(e+1) = e(n+1)$. Since $e \mid y_j(e+1)$, $y_j(e+1) \equiv j \pmod{e}$, and $j > 0$, $e \leq j$. By the inequalities we derived in the last section,

$$e(e-1) + e^{e-1} < (2(e+1)-1)^e \leq y_e(e+1) \leq y_j(e+1) = e(n+1).$$

from which the first part of the result follows.

The second part comes from the fact that we can find nontrivial solutions (α, γ) to $\alpha^2 - e^3(e+2)\beta^2 \cdot \gamma^2 = 1$. Then we set $n = \beta\gamma - 1$. $\square$

We also need the following result, which is very similar to one we proved earlier in showing factorial to be Diophantine (it can be proved in a similar way as well): For $n \geq (2k)^k$ and $p > n^k$,

$$k! < \frac{(n+1)^k p^k}{\mathrm{rem}((p+1)^n, p^{k+1})} < k! + 1.$$

Then we can give a compact definition of factorial:

Lemma: The set defined by the relation $\epsilon = k!$ $(\alpha, k > 0)$ is a projection of the set defined by:

$$\begin{aligned} q &= wz + h + j \\ z &= \epsilon(h+j) + h \\ (2k)^3(2k+2)(n+1)^2 + 1 &= f^2 \\ p &= (n+1)^k \\ q &= (p+1)^n \\ z &= p^{k+1} \end{aligned}$$

Proof: Note that $(n+1)^k p^k = pz/p = z$, so the factorial inequality given above can now be written $k! < z/\mathrm{rem}(q,z) < k!+1$. Now, suppose we have variables satisfying the equations. Since $q = (p+1)^n$ and $z = p^{k+1}$, z does not divide into q, and by $q = wz + h + j$, $0 \neq (h+j) \neq z$. Furthermore, from $z = \epsilon(h+j)+h$, we have that $h+j < z$, so $h+j = \mathrm{rem}(q,z)$. Then, again from $z = \epsilon(h+j)+h$, $\epsilon \leq z/\mathrm{rem}(q,z) < \epsilon+1$. Since $\epsilon, k!$ are both integers, f must be equal to $k!$.

For the other direction, assume $\epsilon = k!$. We can choose n such that $n \geq (2k)^k$ and the third equation holds (let $\beta = (2k)^k + 1$, for example). Then the last three equations immediately

determine p, q, z. If we set $w = (q - \text{rem}(q, z))/z, h = z - \epsilon \cdot \text{rem}(q, z), j = \text{rem}(q, z) - h$, then the equations will be satisfied. $\square$

We now exhibit a set of equations defining the primes. Specifically, for $k > 0$, $k + 1$ is prime if and only if the following equations are satisfied:

$$
\begin{aligned}
P_1 &: n + l + v = y \\
P_2 &: x^2 - (a^2 - 1)y^2 = 1 \\
P_3 &: u^2 - 16(a^2 - 1)r^2y^4 = 1 \\
P_4 &: (x + cu)^2 - ((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 = 1 \\
P_5 &: m^2 - (a^2 - 1)l^2 = 1 \\
P_6 &: l = k + i(a - 1) \\
P_7 &: (2k)^3(2k + 2)(n + 1)^2 + 1 = f^2 \\
P_8 &: e^3(e + 2)(a + 1)^2 + 1 = o^2 \\
P_9 &: e = p + q + z + 2n \\
P_{10} &: p = m - l(a - n - 1) - b(2a(n + 1) - (n + 1)^2 - 1) \\
P_{11} &: q = x - y(a - p - 1) - s(2a(p + 1) - (p + 1)^2 - 1) \\
P_{12} &: z = pm - pl(a - p) - t(2ap - p^2 - 1) \\
P_{13} &: q = wz + h + j \\
P_{14} &: z = (gk + g + k)(h + j) + h
\end{aligned}
$$

Proposition: Satisfying these equations forces $k + 1$ to be prime.

Proof: Suppose we have variables satisfying the equations. We recognize $P_1 - P_4$ as ensuring that $x = x_n(a)$ and $y = y_n(a)$. Also, the first equation guarantees $l < y$. Then by P_5, there is some $k' < n$ such that $m = x_{k'}(a)$ and $l = y_{k'}(a)$. By P_6, $k \equiv y_{k'}(a) \equiv k' \pmod{a - 1}$

Substituting P_9 and P_8, and applying the "exponential growth" lemma from earlier gives us:

$$(p + q + z + 2n) - 1 + (p + q + z + 2n)^{p+q+z+2n-2} \leq a$$

We can deduce a variety of facts from this equation. First of all, $n < a$. Meanwhile, P_7 guarantees that $k < n$. Thus, both k and k' are less than $a - 1$. implying that $k' = k$ and $m = x_k(a)$ and $l = y_k(a)$.

Also, we have that $p < a$ and $(n + 1)^k < (n + 1)^n < a$. If we start from the inequality $\frac{(n+1)^2+1}{2n+1} < n < a$, then through some algebra, we have $a < 2a(n + 1) - (n + 1)^2 - 1$, so both p and $(n + 1)^k$ are less than the complex expression.

We now need a somewhat odd congruence:

Lemma: $x_\kappa(a) - (a - \delta)y_\kappa(a) \equiv \delta^\kappa \pmod{2a\delta - \delta^2 - 1}$

Proof: We show this by induction. $x_1(a) - (a - \delta)y_1(a) = a - (a - \delta) = \delta$ and $x_2(a) - (a - \delta)y_2(a) = 2a^2 - 1 - 2a(a - \delta) = 2a\delta - 1 \equiv \delta^2 \pmod{2a\delta - \delta^2 - 1}$, so the congruence holds for $\kappa = 1, 2$.

For the inductive step, we note that from the recurrence relations for $x_\kappa(a), y_\kappa(a)$, we can derive that $x_{\kappa+1}(a) = 2ax_\kappa(a) - x_{\kappa-1}(a)$ and $y_{\kappa+1}(a) = 2ay_\kappa(a) - y_{\kappa-1}(a)$. Thus, $x_{\kappa+1}(a) - (a - \delta)y_{\kappa+1}(a) = 2ax_\kappa(a) - x_{\kappa-1}(a) - (a - \delta)[2ay_\kappa(a) - y_{\kappa-1}(a)] = 2a[x_\kappa(a) - (a - \delta)y_\kappa(a)] - (x_{\kappa-1}(a) - (a - \delta)y_{\kappa-1}(a))$.

By the inductive hypothesis, this last expression is $\equiv 2a\delta^\kappa - \delta^{\kappa-1} \equiv \delta^{\kappa-1}(2a\delta - 1) \equiv \delta^{\kappa-1}\delta^2 \equiv \delta^{\kappa+1} \pmod{2a\delta - \delta^2 - 1}$. $\square$

Putting in $\delta = n+1$ and $\kappa = k$, then making the m, l substitutions gives us $m - (a-n-1)l \equiv (n+1)^k \pmod{2a(n+1) - (n+1)^2 - 1}$. By P_{10}, we have $p \equiv (n+1)^k \pmod{2a(n+1) - (n+1)^2 - 1}$. Combined with the known inequalities, we conclude $p = (n+1)^k$.

In completely analogous fashion, using P_{11} and putting in $\delta = p+1$, we have $q = (p+1)^n$.

From $\delta = p$, we get the result $m - l(a-p) \equiv p^k \pmod{2ap - p^2 - 1}$. Combined with P_{12}, we have $z \equiv p^{k+1} \pmod{2ap - p^2 - 1}$. Since z obeys inequalities analogous to those for p and q, $z = p^{k+1}$.

Thus, the final three equations for the Diophantine definition of factorial are satisfied (by the same-named variables p, q, z, n, k). P_7, P_{13} are exactly the third and first of those equations, respectively, and by P_{14}, letting $\epsilon = gk + g + k$ gives us the second equation. This is all of them; therefore, $gk + g + k = k!$.

Then $k! + 1 = gk + g + k + 1 = (g+1)(k+1)$, so $k+1 \mid k! + 1$. By Wilson's Theorem, $k+1$ is prime. $\square$

Proposition: If $k+1$ is prime, then there is a solution to $P_1 - P_{14}$.

Proof: (This is basically the reverse of the previous proof but is much easier.) By Wilson's Theorem, $k+1 \mid k! + 1$, so there is a g such that $k! + 1 = (g+1)(k+1)$. By the Diophantine nature of factorial, we can choose f, h, j, n, p, q satisfying P_7, P_{13}, P_{14} as well as $p = (n+1)^k, q = (p+1)^n, z = p^{k+1}$. Choose e so that P_9 is satisfied. By the "exponential growth" lemma, we can choose a, o so that P_8 is satisfied. By the Diophantine nature of $y_n(a)$, x, y, m, l (as well as c, d, r, u) can be found to satisfy $P_2 - P_5$. i is then chosen to satisfy P_6.

By induction, we can show that $n + y_{n-1}(a) \leq y_n(a)$, so in particular, $n + l = n + y_k(a) \leq y_n(a) = y$ ($k < n$ from P_7). Thus, we can have a v satisfying P_1.

$P_{10} - P_{12}$ remain. But by the congruence lemma shown in the proof of the other direction, we can find b, s, t satisfying $P_{10} - P_{12}$. (That b, s, t are nonnegative is shown as follows: We can prove that for $\delta^n < a$, we have $x_n(a) \geq \delta^n + (a-\delta)y_n(a)$, since $x_n(a) > y_n(a)\sqrt{a^2-1}$. But we know $(n+1)^k < a, (p+1)^n < a, p^k < a$, so the result follows.). $\square$

With that proved, we can apply the trick alluded to at the beginning of this section of expressing each of $P_1 - P_{14}$ as an equation with 0 on one side, then taking the sum of the squares of the resulting polynomials, subtracting it from 1, and multiplying the resulting expression by $k+1$. However, since the condition on k is currently that it must be strictly greater than 0, the slight adjustment of substituting $k+1$ for k everywhere is required to make sure the result holds as all the variables range over the nonnegative integers. Explicitly, the set of prime numbers coincides with the set of positive values assumed by polynomial:

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

(as its variables range over the nonnegative integers)

Though the polynomial may seem somewhat unwieldy, it was not known that it was possible

to exhibit such a prime-defining polynomial until Matiyasevich showed the Diophantine nature of exponentiation in 1970. In fact, before the Matiyasevich result, there was no known method for proving a number to be prime in a bounded number of steps that did not depend at all on the number being tested. The equations $P_1 - P_{14}$ will provide such a proof, i.e., since satisfying $P_1 - P_{14}$ proves $k + 1$ is prime, we need only make the 87 additions and multiplications of those equations in order to check $k + 1$'s primality. This, of course, is of no use in the search for primes because in addition to k, we need to know appropriate $a, b, c, \ldots, j, l, \ldots, y, z$ in advance to calculate the check. Still, it is a result of great aesthetic value.

6 References

Z. Adamowicz and P. Zbierski.
[1997] *Logic Of Mathematics: A Modern Course of Classical Logic*, John Wiley & Sons, New York.

M. Davis.
[1973] Hilbert's tenth problem is unsolvable, *American Mathematical Monthly*, **80**, 233–269.

M. Davis, H. Putnam, and J. Robinson.
[1961] The decision problem for exponential Diophantine equations, *Annals of Mathematics*, **74**, 425–436.

J. P. Jones, D. Sato, H. Wada, and D. Wiens.
[1976] Diophantine representation of the set of prime numbers, *American Mathematical Monthly*, **83**, 449–464.

S. C. Kleene.
[1943] Recursive predicates and quantifiers, *Transactions of the American Mathematical Society*, **53**, 41–73.

Y. I. Manin.
[1977] *A Course in Mathematical Logic*, Springer-Verlag, New York.

Y. V. Matiyasevich.
[1993] *Hilbert's Tenth Problem*, MIT Press, Cambridge.

J. Robinson.
[1952] Existential definability in arithmetic, *Transactions of the American Mathematical Society*, **72**, 437–449.

R. I. Soare.
[1987] *Recursively Enumerable Sets and Degrees*, Springer-Verlag, New York.