Bachelor's Thesis:

Diophantine representations of recursive enumerable sets

Niels Voorneveld

Student number: 3632288

Utrecht University

July 3, 2013

Supervisor: Prof. Dr. Frits Beukers

Universiteit Utrecht

Abstract

In this thesis we will discuss various results found by other mathematicians about the connection between recursively enumerable sets and diophantine representation. As a starting point, we will use the Martin Davis theorem that uses results from Gödel and Rosser. We will then review the proofs of the DPR-theorem, the DPRM-theorem and the single-fold DPR-theorem. After that, we will discuss the conjecture that all recursively enumerable sets are single-fold diophantine. A main result discussed in this thesis is the diophantine representation of the exponential relation found by the mathematician Matiyasevich. A single-fold diophantine representation of this same relation would prove the conjecture, but this has not been found yet. There is a result that a non-effective estimate of the solutions of the equation $9(u^2+7v^2)^2-7(r^2+7s^2)^2=2$ would theoretically give us a single-fold diophantine representation of exponentiation. We will look at the proof of this statement and we will study some solutions of other equations like the one in the statement.

Contents

1 Introduction

1.1 Hilbert's wish

A diophantine equation is an equation of the form:

$$D(x_1, x_2, ..., x_n) = 0 \tag{1}$$

Where $D(x_1, x_2, ..., x_n)$ is a polynomial with integer coefficients and integer unknowns x_1, x_2,... x_n.
Solving equations of this type has been a challenge for mathematicians from the moment the ancient Greek philosopher Diophantus conceived its structure. Many specific examples of those equations have been thoroughly studied and the names of countless of those mathematicians are used to refer to these equations. By 1900, many a field in mathematics had been lifted from mysterious conjecture to the realm of the proven, but the solvability of the Diophantine equation was one problem that had remained open.
The German mathematician David Hilbert came to the mathematical congress on the first year of the new century to inspire the people of the new age to try and solve the still unsolved. He hand-picked 23 problems to present to his audience, and among those 23 there was a particularly famous one, Hilbert's tenth. In this problem Hilbert asked the people if there was a way to determine that an arbitrary diophantine equation had a solution or not. He probably hoped the answer was yes, but he did not live long enough to find out that in fact the answer was no. After 70 years, a Russian mathematician named Matiyasevich did what had seemed impossible, with help of the work of his predecessor's Julia Robinson, Martin Davis and Robert Putnam, he was able to close the final gap in the theorem that solved Hilbert's problem (published in [8]):

DPRM-theorem *Every recursively enumerable relation is diophantine*

Let us first discuss what this theorem means and why it ruined the hope of some that maybe some day all diophantine equations could be solved. A relation of rank n on $\mathbb{Z}$ is a subset of $\mathbb{Z}^n$. When can we call such a relation diophantine? Let us consider a rank n relation and call it A. We say that A is represented by a diophantine equation $D(x_1, x_2, ..., x_k) = 0$ in $k = n + r$ variables if for every element $(a_1, a_2, ..., a_n)$ of A there is a solution of $D = 0$ with $a_1, a_2, ..., a_n$ as its first n coördinates and for every solution of $D = 0$ it's first n coördinates form an element of A. The formal definition being:

Diophantine representation: The relation A is represented by $D\epsilon\mathbb{Z}[a_1, ..., a_n, x_1, ..., x_r]$ if: $((a_1, a_2, ..., a_n)\epsilon A) \Leftrightarrow (\exists x_1 x_2 ... x_r \epsilon\mathbb{Z})[D(a_1, a_2, ..., a_n, x_1, x_2, ..., x_r) = 0]$

An alternate equivalent definition could be that A is represented by $D\epsilon\mathbb{Z}[a_1, ..., a_n, x_1, ..., x_r]$ if it is the projection of the solution space of the equation $D(a_1, ..., a_n, x_1, ..., x_r) = 0$ on the first n coördinates.
If a relation $A \subset \mathbb{Z}^n$ is represented by some diophantine equation, we call it Diophantine.
Now let us discuss the concept of a recursive enumerable relations. One says a relation is recursively enumerable (in short r.e.) if it is empty or the exact range of some recursive functions. This means that the relation $A \subset \mathbb{Z}^n$ has an algorithm which takes an element from $\mathbb{Z}^n$ and when that element is in A it stops to tell us that it is in A. The problem is that such an algorithm does not need to stop if the element is not in A, and it can run an infinite amount of time if this is the case.
A relation is called recursive if there is an algorithm which will always stop and tell whether or not the element is in the set. An alternate definition might be that a relation A is recursive if A and its complement are both recursive enumerable. The definition of recursive sets is stronger than the definition of r.e. sets as it has been proven that there are recursive enumerable relations with a non-recursive enumerable complement.

Hilbert's tenth problem could be seen in terms of recursiveness, he asked for an algorithm to determine if an arbitrary diophantine equation has a solution or not. This would imply that every diophantine set is recursive. But that statement was refuted when they found the proof of the DPRM theorem. Any recursively enumerable set is diophantine, so even those sets that are not recursive. This gives us a contradiction and Matiyasevich concluded that Hilbert's tenth problem had a negative answer.

1.2 Endless complexity

So ends the tenth problem of Hilbert. This conclusion may have disappointed Hilbert himself if he were still alive. So it does not matter how long we try to study the structures flowing from our axioms, there will always be diophantine equations that are yet to be solved. Our mathematics is infinitely complex and there will always be areas to discover for those who seek the uncharted.

One of those open problems yet in the realm of the conjectures is found in the proof of the DPRM-theorem. Before 1970, a big part of the theorem was already proven in the shape of the weaker version (in [6]):

DPR-theorem: *Every recursively enumerable relation is exponentially diophantine*

Did you see the difference? It was the word 'exponentially' in front of the word 'diophantine'. The concept of an exponential diophantine equation is the idea that we can use unknowns in the exponents. To give a more specific definition, we will first look at a definition of integral polynomials. The set A_n is the set containing all polynomials with at most n unknowns $(x_1, x_2, ..., x_n)$ if it is generated by the following rules:
• $x_1 \epsilon A_n$, $x_2 \epsilon A_n$,...,$x_n \epsilon A_n$. So any unknown itself is an integral polynomial.
• For all constants $a \epsilon \mathbb{Z}$, $a \epsilon A_n$.
• If $P_1 \epsilon A_n$ and $P_2 \epsilon A_n$, then $(P_1 + P_2) \epsilon A_n$.
• If $P_1 \epsilon A_n$ and $P_2 \epsilon A_n$, then $(P_1 P_2) \epsilon A_n$.
The smallest set obeying all of these rules is the set containing all polynomials of at most n unknowns, so a function with n unknowns is a polynomial if and only if it is a subset of A_n.
We can now define the set E_n of exponential polynomials with at most n unknowns as the smallest set obeying the same rules as before, but with an added rule of:
• If $P_1 \epsilon E_n$ and $P_2 \epsilon E_n$, then $(P_1^{P_2}) \epsilon E_n$.
So a set $A \subset \mathbb{Z}^n$ is exponentially diophantine if for some $k \geq n$ there is an element $D(x_1, ..., x_k) \epsilon E_k$ such that for all $(y_1, ..., y_n) \epsilon \mathbb{Z}^n$, $x \epsilon A \Leftrightarrow (\exists x_1 x_2 ... x_{k-n} \epsilon \mathbb{Z})[D(y_1, ..., y_n, x_1, ..., x_{k-n}) = 0]$.

You can imagine that we can represent relations much easier with exponential diophantine equations than with diophantine equations. As the differences in the theorems suggests, the last step that was done to prove the DPRM-theorem was the fact that every exponentially diophantine relation was in fact also diophantine, and this was proven by Y.U. Matiyasevich. He proved that exponentiation itself can actually be represented by a diophantine equation, by proving that the following relation is diophantine:

$$\{< a, b, c > \epsilon \mathbb{Z}^3 | a = b^c\} \tag{2}$$

Using this one could switch all variable exponents from the exponentially diophantine representations using this specific representation to find the diophantine representation of a specific recursively enumerable relation.
After this proof, another improvement of the DPR-theorem was made but in another direction ([8]):

The single-fold DPR-theorem: *Every recursively enumerable relation is single-fold exponen-*

tially diophantine

This time, adding a word actually made the theorem stronger. A relation that is single-fold exponentially diophantine means that there is an exponential diophantine equation which not only represents the relation but also only has one solution per element of the relation.
As of now we are not able to translate this single-foldness to the DPRM-theorem. Thus it still remains to be proven or disproven that every recursively enumerable relation is single-fold or even finite-fold diophantine (finite-fold meaning there are only a finite number of solutions per element of the relation). But because of the before-mentioned other improvement of the DPR-theorem it is sufficient to prove that the relation in (2) is diophantine in a single-fold (or finite-fold, depends on what you want) way. Let us state the weakest form of this conjecture:

Main Conjecture (Open problem): $\{< a, b, c > \epsilon \mathbb{Z}^3 | a = b^c\}$ *is finite fold diophantine*

Interestingly enough, an earlier attempt to close the final gap in DPRM-theorem made by Martin Davis ([7]) had this single-foldness. So it was disappointing to discover that the extra assumption he made in his proof was actually not true. He assumed that the following equation:

$$9(u^2 + 7v^2)^2 - 7(r^2 + 7s^2)^2 = 2 \tag{3}$$

only had the trivial solution $u = 1, v = 0, r = 1, s = 0$. A weaker form of this assumption could be used to ward of the finiteness of the diophantine representability (In other words, it could be used to prove the aforementioned conjecture) but its truth remains to be proven. Using Martin Davis original proof and this weaker version of the assumption, one can state the following fact:

Salvaged Martin Davis theorem *If (3) has finitely many solutions then the Main Conjecture is true.*

Of course there is always the possibility that the assumption may not be true at all.

Let us step back from all this for a moment. Notice that Davis' assumption actually entails the solvability of a certain diophantine equation (if you remove two from both sides of the equation). So the finiteness of diophantine representations of an arbitrary r.e. relation can be reduced to finiteness of solutions of a specific equation. On the other hand, the fact that we still do not know if this equation has finite solutions is actually a testimony of the mysteriousness of the insolvability of diophantine equations in general. In fact, this equation might actually be a specific example of the falseness of Hilbert's tenth problem.

In this paper we will look at the proof of the DPR-theorem, the DPRM-theorem and the single-fold DPR-theorem. We will also discus how far we are from proving the main conjecture. But we will first dive deeper into the concepts of diophantine representability and recursive enumerability in the next two chapters.

2 Diophantine equations

2.1 Definitions

A diophantine equation can be described as a integer polynomial which must be equal to zero. So if we have a set of n variables, say $a_1, a_2, ..., a_n$, we may combine them with summation and

multiplication, and scale them with integer values. This lets us create arbitrary integer polynomials such as $P(a_1, a_2, a_3) = 5(a_1 + 2a_2) - a_2(3a_3 - a_1)^2$.
If we now take $P(a_1, a_2, a_3) = 0$ and also demand the variables to be integer, we have created a diophantine equation. Notice that demanding the variables to be integer severely diminishes the number of possible solutions.
Take for instance the famous equation of pythagoras $a^2 + b^2 = c^2$. This equation is satisfied by the lengths of the sides of any right-angled triangle, but if we demand a, b and c to be integer, there are far less solutions possible. So much less, that if we look at a specific Fermat equation $a^4 + b^4 = c^4$, we find that it has no positive integer solution at all, while in the real numbers you can just take the square root of the sides of a right angled triangle.
So it is difficult to judge the nature of the solutions of diophantine equations. Each new one can provide a new challenge. Of course, certain types of Diophantine equations have been studied extensively, and a lot is known about them. We for instance know a lot about elliptic curves, linear diophantine equations and quadratic forms. Unfortunately, these studies limit themselves to equations with a maximum power smaller than 4. Why is this a problem? Because we will be facing equations with much higher powers and much more variables before this paper is over.

So how do we want to use these types of equations? As was discussed before, we want to describe sets with them. Take an n-placed integer relation A (a subset of $\mathbb{Z}^n$), and an integer polynomial $D(a_1, a_2, ..., a_n, x_1, x_2, ..., x_r) = 0$. As defined before we can say that a relation A is represented by $D = 0$ if for all $(a_1, a_2, ..., a_n) \epsilon \mathbb{N}^n$: $((a_1, a_2, ..., a_n) \epsilon A) \Leftrightarrow (\exists x_1, x_2, ...x_r)[D(a_1, a_2, ..., a_n, x_1, x_2, ..., x_r) = 0]$.
This is called a diophantine representation. With $D = 0$ we can check the contents of A.
So take for instance again the pythagoras equation $D(c, a, b) = c^2 - a^2 - b^2 = 0$ and we define $A \subset \mathbb{Z}$ by the statement that $c \epsilon A$ if and only if there are integers b and c such that $D(c, a, b) = 0$. Then A is diophantine and in this example it is exactly the set of all possible hypothenuse of right angled triangles with sides of integer length.

Besides normal diophantine equations, we can also define exponential ones. These allow the use of variable exponentiation, meaning they have actual variables in the exponents. Of course any diophantine equation is automatically also an exponential diophantine equation, because variable exponents are allowed but not demanded. The same way as with regular diophantine equations, we can define exponential diophantine relations as integer relations that can be represented by an exponential diophantine equation in much the same way as before. So a relation $A \subset \mathbb{Z}^n$ which satisfies $((a_1, a_2, ..., a_n) \epsilon A) \Leftrightarrow (\exists x_1 x_2 ... x_r)[D(a_1, a_2, ..., a_n, x_1, x_2, ..., x_r) = 0]$ with $D = 0$ an exponential diophantine equation, is called exponential diophantine.

When talking about diophantine equations, one can also discuss the number of solutions it has. The equations can be called single-fold, finite-fold and infinite-fold. Single-fold if it only has one solution, finite-fold if the number of solutions is finite and infinite-fold otherwise. This can also be used to describe diophantine representations. For instance, an n-tuple relation A is called single-fold diophantine if for every $(a_1, a_2, ..., a_n) \epsilon \mathbb{Z}^n$, $((a_1, a_2, ..., a_n) \epsilon A) \Leftrightarrow (\exists! x_1, x_2, ...x_r) : [D(a_1, a_2, ..., a_n, x_1, x_2, ..., x_r) = 0]$, with $D = 0$ a diophantine equation. Here the quantifier $\exists! x$ means: *there is an unique variable x such that.*
In the same way, finite-fold diophantine means there is a diophantine equation which only has a finite number of solutions per element of A. Of course, the same story goes for defining single-fold or finite-fold exponential diophantine relations.

2.2 Natural sets

We have talked about the diophantine equations with integer variables. But we can also talk about these types of equations with non-negative variable, meaning they are elements of the natural set $\mathbb{N} = \mathbb{Z}_{\geq 0}$. Take for instance an arbitrary equation $D(a_1, a_2, ..., a_n) = 0$ with integer unknowns. Notice that for each $1 \leq i \leq n$ we can define a new equation $P(a_1, a_2, ..., a_{i-1}, b_i, c_i, a_{i+1}, ..., a_n) = D(a_1, a_2, ..., a_{i-1}, b_i - c_i, a_{i+1}..., a_n) = 0$ with the b_i and c_i natural unknowns. Because $b_i - c_i$ can reach all integers (the domain of a_i in the original equation) we can conclude that $D(a_1, a_2, ..., a_n) = 0$ has a solution if and only if $P = 0$ has a solution. So we have successfully replaced the integer a_i with two natural numbers.
For the other way around, we go back to a classic theorem:

Lagrange (1770): *Every non-negative integer can be written as the sum of four squares*

So if we have a diophantine equation $P(a_1, a_2, ..., a_n) = 0$ with all a_i natural numbers, we can define an equation with integer variables as follows $D(a_1, a_2, ..., a_{i-1}, b_i, c_i, d_i, e_i, a_{i+1}, ..., a_n) := P(a_1, a_2, ..., a_{i-1}, b_i^2 + c_i^2 + d_i^2 + e_i^2, a_{i+1}, ..., a_n) = 0$ and conclude that $P = 0$ has a solution if and only if $D = 0$ has a solution. So the natural variable a_i has been replaced by four integer variables.

So what does that mean? If we have a relation A that is diophantine, we know that there is an integral polynomial $D(a_1, a_2, ..., a_n, x_1, x_2, ..., x_r)$ such that $((a_1, a_2, ..., a_n) \epsilon A) \Leftrightarrow (\exists x_1, x_2, ...x_r)[D(a_1, a_2, ..., a_n, x_1, x_2, ..., x_r) = 0]$. But with what we have found before, it is possible to replace all the x_i's with natural variables, constructing $P(a_1, a_2, ..., a_n, y_1, y_2, ..., y_r, z_1, z_2, ..., z_r) := D(a_1, a_2, ..., a_n, y_1 - z_1, y_2 - z_2, ..., y_r - z_r)$ such that $((a_1, a_2, ..., a_n) \epsilon A) \Leftrightarrow (\exists x_1 \geq 0, x_2 \geq 0, ...x_{2r} \geq 0)[P(a_1, a_2, ..., a_n, x_1, x_2, ..., x_{2r}) = 0]$, so A is represented by a diophantine equation with natural variables (of course the elements of the set can still have negative elements). And using the other method, any relation represented by a diophantine equation with only natural unknowns can also be represented by an equation with integer unknowns.
So in diophantine representability, it does not matter if the variables are integers or natural numbers. So from this moment on,

We will assume all parameters and unknowns to be natural unless it is specifically stated otherwise.

This will also be the case for our relations. Any n-tuple relation will thus be an element of $\mathbb{N}^n$.

Speaking of relations, it is not necessary to make a distinction between n-tuple relations and 1-tuple relations. Not only does there exist a bijection between $\mathbb{N}$ and $\mathbb{N}^n$, and between $\mathbb{Z}$ and $\mathbb{Z}^n$, it is also possible to describe this map in a single-fold diophantine way. This diophantine map will be discussed in chapter 9. For now, it is sufficient to know that:

For all n, all integral recursive enumerable n-tuple relations are (single-fold) (exponential) diophantine representable if and only if all recursive enumerable subsets of $\mathbb{N}$ are (single-fold) (exponential) diophantine representable.

2.3 Simple diophantine relations

Now for some specific relations. Firstly, when we have two relations A and B of rank n represented by the diophantine equations $D_1(a_1, a_2, ..., a_n, x_1, x_2, ..., x_r) = 0$ and $D_2(b_1, b_2, ..., b_n, y_1, y_2, ..., y_l) = 0$, we

can represent their intersection $C = A \bigcap B$ with the equation:

$$D_1(c_1, c_2, ..., c_n, x_1, x_2, ..., x_r)^2 + D_2(c_1, c_2, ..., c_n, y_1, y_2, ..., y_l)^2 = 0 \tag{4}$$

This is because we know that the only solution of $x^2 + y^2 = 0$ is the trivial one. Notice that this new equation does not eliminate possible single- or finite-foldness of $D_1 = 0$ and $D_2 = 0$. This method is very handy, with it we can conclude that the solutions of any system of multiple diophantine equations are the same as the solutions of a certain single diophantine equation. Many a time we will discuss a system of diophantine equation because they are actually easier to consider.
With D_1 and D_2 we can also represent their union $C = A \bigcup B$ by:

$$(D_1(c_1, ..., c_n, x_1, ..., x_r)^2 + y_1^2 + ... + y_l^2)(D_2(c_1, ..., c_n, y_1, ..., y_l)^2 + x_1^2 + ... + x_r^2) = 0 \tag{5}$$

By using the x-s and y-s outside the D_1 and D_2 we are able to conserve single-foldness if A and B are disjoint.
If we do not need the single-fold property, we can also just simply use the product $D_1(c_1, ..., c_n, x_1, ..., x_r)D_2(c_1, ..., c_n, y_1, ..., y_l) = 0$ as the representation.

For the next few relations, remember we assumed all variables to be non-negative, so all variable are elements of $\mathbb{N} = \mathbb{Z}_{\geq 0}$. So:

$$a \leq b \Leftrightarrow \exists x : [a + x = b] \tag{6}$$

$$a < b \Leftrightarrow \exists x : [a + x + 1 = b] \tag{7}$$

$$a \neq b \Leftrightarrow \exists x : [(a - b)^2 = x + 1] \tag{8}$$

$$a|b \Leftrightarrow \exists x : [ax = b \quad \& \quad x \leq b] \tag{9}$$

These relations are also all single-fold. Notice that in the last one, we added the relation $x \leq b$ in order to eliminate the infinite number of possibilities for x when $a = b = 0$. Notice that we can freely use the symbol '&' because of (4).

With help of (9) we can create some more single-fold relations, where we define $rem(a, b)$ as the remainder of dividing a by b:

$$c = rem(a, b) \Leftrightarrow c < b \quad \& \quad b|(a - c) \tag{10}$$

$$a \not| \ b \Leftrightarrow rem(b, a) > 0 \tag{11}$$

$$(a \equiv b) mod(c) \Leftrightarrow rem(a, c) = rem(b, c) \tag{12}$$

When using exponential diophantine representations, it is possible to create rational numbers which are not integer. This will happen when there are negative numbers in the exponents. That is why this next diophantine relation will come in handy, for a rational non integers a and b:

$$b = entier(a) \Leftrightarrow \exists x, y, z, w[(xa + y = xb) \quad \& \quad (zb + w = z(a + 1))] \tag{13}$$

Last but not least we will define $GPT(a)$ for each integer a as the greatest power of 2 which divides a. With this we can create the relation:

$$a \geq GPT(b) \Leftrightarrow (\exists x, y) : [b = y(2x + 1) \quad \& \quad a \geq y] \tag{14}$$

3 Recursively enumerable relations

Let us now study the concept recursive enumerable relations and its connection to integral polynomials. In the 1930s, a new branch in mathematical logic was perceived called recursion theory, later to be renamed computability theory. In the beginning stages two concepts arose, recursive sets and recursive enumerable sets. Both types are subsets of the natural numbers. Tightly linked together, they both can be defined by a function that tells us in a finite amount of time if a certain number is in the set. Recursiveness also demands that the function will always give his answer in a finite amount if time. Recursive enumerability does not care if the function might never stop computing if the number is not in the set. This means that you might never know for certain if a number is not in the set.
Let us give some formal definitions:

Recursive set: A subset S of the natural numbers is called recursive if there is a computable function over the natural numbers that gives 1 to all numbers in S and 0 to all numbers not in S.

Recursive enumerable set: A subset S of the natural numbers is called recursive enumerable if there is a computable function f which is defined over S, so its domain is S.

We see the word computable turn up in both of these definitions. Originally, the idea of computable functions is that you can build a machine, for instance a Turing machine, to calculate the outcome of the function. Of course, machines being a physical thing and the physical world being far from formally defined, it is difficult to give the concept a place in mathematics. It is also possible to look at computability in an effectively intuitive sense, meaning that you can define it with logical steps in your head, this is called effectively calculable.
The mathematician Church stated that these two things, effectively calculable and computable by machines are equivalent, creating something that is very uncommon in mathematics, a thesis. This means that it can never be really proven.
Though the definition may be vague, a lot of concrete examples can be given. In short, one can say that any subset of the natural numbers you can think of (still obeying axioms of set theory of course) is recursive enumerable.

But how do you connect these concepts to something so concrete as exponential diophantine equations? This can be done by combining two mayor results in computability theory.
The first one was by Gödel [2]. He talked about *polynomial* and *arithmetic* predicates. A polynomial predicate is an equation $P = Q$ with P and Q both integral polynomials. The predicate gives us truth (1) if the equation is true and false (0) if the equation is not valid. An arithmetic predicate is a polynomial predicate with a finite number of universal and existential quantifiers in front of it. Gödel proved that any primitive recursive predicate is also immediately arithmetic. Not only that, in his result all his universal quantifiers were bounded. So he did not use $(\forall z)$, only $(\forall z < k)$ with k some constant.
The other result was by Rosser [3]. He proved that any recursively enumerable predicate can be written as a primitive recursive predicate with one existential predicate. Combining these two results one gets that:

Gödel and Rosser: *Any recursively enumerable set can be represented by an arithmetic predicate with existential quantifiers and bounded universal quantifiers*

Martin Davis took it upon himself (in [5]) to try and reduce the quantifiers in front of the polynomial predicate and succeeded. Combining this with the result of Gödel and Rosser Martin was

able to prove the following theorem:

Davis' theorem: *For every recursively enumerable subset $A \subset \mathbb{Z}$ there is an integral polynomial $P(a_1, ..., a_{m+3}) \epsilon \mathbb{N}[a_1, ..., a_{m+3}]$ such that for all $x \epsilon \mathbb{N}$: $x \epsilon A \Leftrightarrow (\exists y)(\forall k \leq y)(\exists z_1 \leq y ... \exists z_m \leq y) P(x, y, k, z_1, ..., z_m) = 0$.*

Notice that a diophantine predicate is a polynomial predicate with only existential quantifiers in front of it. So with this result, we seem to be quite close to proving that all recursively enumerable sets are diophantine, but the universal quantifier, though bounded, forces us to use exponentiation. In the next chapter we look at a proof of the first major theorem.

4 Proof of the DPR-theorem

We have discussed two major concepts, (exponential) diophantine relations and recursively enumerable relations. We will now look at the first bridge between the two. First published in 1961 ([6]) by three prominent experts in the field was the connection between recursive enumerable and exponential diophantine:

DPR theorem: *Every recursively enumerable relation is exponential diophantine*

In this chapter, we will look at its proof.

4.1 Helpful exponential diophantine relations

First remember that all the diophantine relations are of course also exponential relations, so we can use all the relations from chapter 2.3 . Now for some more specific relations in the form of five lemmas. The first two lemmas lend themselves from [4], and the rest are from [6].

Lemma 4.1: *The relation $c = \binom{a}{b}$ with parameters $a, b, c \epsilon \mathbb{N}$, $a > 0$, is single-fold exponential diophantine.*

Proof:
Assume $b > 0$ (because for $b = 0$ we have $\binom{a}{b} = 1$, so the relation is trivially diophantine). Then $2^{ab}(1 + 2^{-a})^a = 2^{ab}(\sum_{n=0}^{a} \binom{a}{n} 2^{-an}) = \sum_{n=0}^{a} \binom{a}{n} 2^{a(b-n)} = \sum_{n=0}^{b} \binom{a}{n} 2^{a(b-n)} + \sum_{n=b+1}^{a} \binom{a}{n} 2^{a(b-n)} < \sum_{n=0}^{b} \binom{a}{n} 2^{a(b-n)} + (\sum_{n=b+1}^{a} \binom{a}{n})/2^a < \sum_{n=0}^{b} \binom{a}{n} 2^{a(b-n)} + (\sum_{n=0}^{a} \binom{a}{n} - 1)/2^a = \sum_{n=0}^{b} \binom{a}{n} 2^{a(b-n)} + (2^a - 1)/2^a < \sum_{n=0}^{b} \binom{a}{n} 2^{a(b-n)} + 1$
And of course $2^{ab}(1 + 2^{-a})^a > \sum_{n=0}^{b} \binom{a}{n} 2^{a(b-n)}$. So $entier(2^{ab}(1 + 2^{-a})^a) = \sum_{n=0}^{b} \binom{a}{n} 2^{a(b-n)}$.
In the same way, we have $2^a entier(2^{a(b-1)}(1 + 2^{-a})^a) = \sum_{n=0}^{b-1} \binom{a}{n} 2^{a(b-n)}$. So we can conclude that $(\binom{a}{b}) = entier(2^{ab}(1 + 2^{-a})^a) - 2^a entier(2^{a(b-1)}(1 + 2^{-a})^a)$, so it is exponential diophantine.

□

Lemma 4.2: *$c = a!$ is single-fold exponential diophantine in parameters a and c.*

Proof:
Notice that for $r > (2a)^{a+1}$, $r^a / \binom{r}{a} = a!/((1 - 1/r)(1 - 2/r)...(1 - (a - 1)/r)) < a!/((1 - a/r)(1 - a/r)...(1 - a/r)) = a!/(1 - a/r)^a < a!(1 + 2a/r)^a < a!(1 + 2^a 2a/r) < a! + 1$.
And of course, $r^a / \binom{r}{a} = a!/((1 - 1/r)(1 - 2/r)...(1 - (a - 1)/r)) > a!$. So $a! = entier(r^a \binom{r}{a}^{-1})$, and we

can conclude that it is single-fold diophantine because both the entier function and the binomials are single-fold exponential diophantine.

□

Lemma 4.3: *$[x/y = \binom{p/q}{k} \quad \& \quad p > qk]$ is single-fold exponential diophantine in parameters x, y, p, q and k.*

Proof:
Take $\alpha = p/q$ and $\alpha > k$. Then we know that there are real numbers θ, θ' between 0 and 1 such that:

$$a^{2k+1}(a+a^{-2})^{\alpha} = \sum_{j=0}^{k} \binom{\alpha}{j} a^{2k-2j+1} + \binom{\alpha}{k+1} a^{-1}(1+\theta a^{-2})^{\alpha-k-1} = S_k(a) + \theta' \alpha^{k+1} a^{-1} 2^{\alpha-1}$$

With $S_k(a) = \sum_{j=0}^{k} \binom{\alpha}{j} a^{2k-2j+1}$.
If $q^k k!$ divides a, then both $S_k(a)$ and $S_{k-1}(a)$ are integers. This is because $\binom{p/q}{j}$ already divides $q^k k!$ for all $j \leq k$. Also, if $a > 2^{p-1}p^{k+1}$ then $\theta' \alpha^{k+1} a^{-1} 2^{\alpha-1}$ is less than 1. So if we choose $a = 2^p p^{k+1} q^k k!$ then we have:
$S_k(a) = entier[a^{2k+1}(1+a^{-2})^{p/q}]$ and $S_{k-1}(a) = entier[a^{2k-1}(1+a^{-2})^{p/q}]$.
So for numbers u, v, p, q, k which satisfy $u = S_k(a)$, $v = S_{k-1}(a)$, we know that $\binom{p/q}{k} = a^{-1}S_k(a) - aS_{k-1}$.

□

From this we can conclude that the binomial coefficient $c = \binom{a}{b}$ with a rational is exponential diophantine.

Lemma 4.4: *The relation $y = \prod_{h \leq H}(a + hb)$ is single-fold exponential diophantine in parameters y, a, b and H.*
Proof: $\prod_{h \leq H}(a+hb) = \binom{a/b+H}{H} b^H H!$, which is clearly diophantine by previous results.

□

4.2 Completing the proof

These were the first four lemmas. Before we continue, remember the theorem discussed in the last chapter:

Davis' theorem: *For every recursively enumerable subset $A \subset \mathbb{Z}$ there is an integral polynomial $P(a_1, ..., a_{m+3}) \epsilon \mathbb{N}[a_1, ..., a_{m+3}]$ such that for all $x \epsilon \mathbb{N}$: $x \epsilon A \Leftrightarrow (\exists y)(\forall k \leq y)(\exists z_1 \leq y ... \exists z_m \leq y) P(x, y, k, z_1, ..., z_m) = 0$.*

With that in mind, we can finish the proof with the next lemma.

Lemma 4.5: *Let $P(x, y, k, z_1, ..., z_m)$ be an integer polynomial and $G(x, y)$ a polynomial with $\forall x, y : G(x, y) \geq y$ and $(\forall x \forall y \forall k \leq y \forall z_1 \leq y ... \forall z_m \leq y) : [|P(x, y, k, z_1, ..., z_m)| \leq G(x, y)]$ then we have for all y:*

$$(\forall h \leq y)(\exists z_1 \leq y ... \exists z_m \leq y) : [P(x, y, h, z_1, ..., z_m) = 0] \Leftrightarrow$$
$$(\exists c, t, a_1, ..., a_m)[t = G(x, y)! \quad \& \quad (1 + ct) = \prod_{k \leq y}(1 + tk) \quad \&$$

$$(1+ct) \mid P(x,y,c,a_1,...,a_m) \quad \& \quad (\forall i \leq m)((1+ct) \mid \prod_{j \leq y}(a_i - j))]$$

We see that all relations on the right hand side are exponential diophantine, as was already discussed. It is also easy to see that for any polynomial $P(x,y,h,z_1,...,z_m)$ we can always find a $G(x,y)$ such that $(\forall x \forall y \forall z_1 \leq y ... \forall z_m \leq y)$: $G(x,y) \geq y$ and $|P(x,y,k,z_1,...,z_m)| \leq G(x,y)$.
We can do this if we define g as the degree of P (at least one) and s as the sum of all absolute values of the coefficients of P and then we see that $G(x,y) = sx^g y^g$ satisfies the conditions.
So combining this choice with the lemma and with Davis theorem, we see that every recursively enumerable set is exponential diophantine. The proof of this lemma uses the Chinese remainder theorem.

Proof of lemma 4.5:
• Let us take an integer x and y and assume there are $c, t, a_1, ..., a_m$ such that:

$$t = G(x,y)!$$

$$\& \quad (1+ct) = \prod_{k \leq y}(1+tk)$$

$$\& \quad (1+ct) \mid P(x,y,c,a_1,...,a_m)$$

$$\& \quad (\forall i \leq m)((1+ct) | \prod_{j \leq y}(a_i - j))$$

Take an arbitrary h lower or equal than y. Now we want to define p_h as an arbitrary prime which divides $(1+ht)$. Define for all natural i, $z_{(h,i)}$ as the remainder of dividing a_i by this prime p_h. We will show that $x, y, h, z_{(h,1)}, ..., z_{(h,m)}$ is a solution of $P = 0$ with $0 < z_{(h,i)} \leq y$.
We know that: for all $i \leq m$, $(1+ct) | \prod_{j \leq y}(a_i - j)$ and $p_h | \prod_{j \leq y}(1+tj) = 1 + ct$.
So $p_h | \prod_{j \leq y}(a_i - j)$ and since p_h is a prime this means there is a j between 1 and y such that $p_h | (a_i - j)$.
So $1 \leq z_{(h,i)} \leq y$ for all i. Because $p_h | (1+ht)$, $gcd(p_h, t) = 1$ and from assumption $t = G(x,y)!$ we can thus derive that $p_h > G(x,y) \geq y$. So we can conclude that $|P(x,y,h,z_{(h,1)},...,z_{(h,m)})| \leq G(x,y) < p_h$.
From our assumption we know that $1 + ct \equiv 0 (mod (1+kt))$, so $c \equiv h (mod (1+th))$ and this means $c \equiv h (mod (p_h))$. Remembering that $a_i \equiv z_{(h,i)} (mod (p_h))$ and that from assumption $(1+ct) | P(x,y,c,a_1,...,a_m)$, whilst $(1+ct) \equiv (1+ht) \equiv 0 \mod p_h$, we can conclude that $P(x,y,h,z_{(h,1)},...,z_{(h,m)}) \equiv P(x,y,c,a_1,...,a_m) \equiv 0 (mod (p_h))$. Which means together with $0 \leq |P(x,y,h,z_{(h,1)},...,z_{(h,m)})| < p_h$ that:

$$P(x,y,h,z_{(h,1)},...,z_{(k,m)}) = 0$$

Which is what we wanted to prove.

• Now, let us prove the theorem the other way. Let us again take natural numbers x and y and now assume that

$$\forall h \leq y (\exists z_1 \leq y ... \exists z_m \leq y) : [P(x,y,h,z_1,...,z_m) = 0]$$

Define $t = G(x,y)!$ and c such that $(1+ct) = \prod_{k \leq y}(1+tk)$ (this is possible because all terms in the expansion of $(\prod_{k \leq y}(1+tk) - 1)$ have a factor t).
So for all k and j $(k \neq j)$ smaller or equal than y, $|(k-j)| \leq y \leq G(x,y)$ and $t = G(x,y)!$, so $(k-j) | t$.
If a prime p divides $(k-j)t$, then this must mean that $p | t$. Thus we find that $gcd(1+kt, 1+jt) = 1$.

Now we use the Chinese Remainder Theorem to find $a_1, ..., a_m$ such that $a_i \equiv z_{(k,i)} \mod (1+kt)$ for all

$k \leq y$ and $i \leq m$. Here we defined $z_{(k,1)}, ..., z_{(k,m)}$ as the solution of $P = 0$ for each k (so also $z_{(k,i)} \leq y$).

Now we have all constants, we only need to show that the rest of the relations on the right hand side of the lemma are valid. We know that $c \equiv k \mod (1 + kt)$ (because $1 + ct \equiv 0$), thus $P(x, y, c, a_1, ..., a_m) \equiv P(x, y, k, z_{(k,1)}, ..., z_{(k,m)}) \equiv 0 \mod (1 + kt)$ for all $k \leq y$. We already proved that $(1 + jt)$ is relative prime for different j, so we know that $P(x, y, c, a_i, ..., a_m)$ is divisible by $(1 + ct) = \prod_{k \leq y}(1 + tk)$, which is the third relation.
From our choice of a_i we have $(1 + kt)|(a_i - z_{(k,i)})$ for all $k \leq y$ and $i \leq m$. This means that $(1 + kt)| \prod_{j \leq y}(a_i - j)$ for all $k \leq y$.
And again, because $(1 + kt)$ is relative prime for all $k \leq y$ we can conclude that $(1 + ct) = \prod_{k \leq y}(1 + kt)| \prod_{j \leq y}(a_i - j)$ for all $i \leq m$. This was the last of the four relations, so now we know that there are $c, t, a_1, ..., a_m$ such that:

$$t = G(x, y)!$$

$$\& \quad (1 + ct) = \prod_{k \leq y}(1 + tk)$$

$$\& \quad (1 + ct) \mid P(x, y, c, a_1, ..., a_m)$$

$$\& \quad (\forall i \leq m)((1 + ct)| \prod_{j \leq y}(a_i - j))$$

This concludes the proof of Lemma 4.5, and as already was discussed, this automatically proves the DPR theorem.

□

We have now seen the proof of the statement that all recursive enumerable sets/relations are exponential diophantine. Next up, proving that they are also diophantine. This can be proven by studying but one relation, exponentiation, and proving that it is diophantine. If we know that we can replace all variable exponents with some integer polynomial creating a diophantine representation from an exponential one. In the next part of this paper, we will look at two attempts to prove this, one failed but can still be used for something else, and one succeeded. But before that, we will look at some important results about the Pell equation.

5 The Pell equation

The Pell equation is a diophantine equation given by:

$$x^2 - dy^2 = 1 \tag{15}$$

Where d is a constant. We always take d to be a non-square, because if d was a square the only solution would be $x = 1$ and $y = 0$. It was known for a long time that the solutions of the Pell equation for a non-square d have an exponential behavior. This meant that the higher you get, the less dense the solutions become. That would make it the ideal choice to try and prove that exponentiation is diophantine. That is why both Davis and Matiyasevich used it in their proofs.
This chapter will be about the properties of the solutions of this type of equations. Most of the information in this chapter is from [7] and [13].

5.1 The specific solutions of the Pell equation

The trivial solution is given by $(1,0)$. To study the non-trivial solutions we will consider the domain $\mathbb{Z}[\sqrt{d}]$ which is the set of integers extended with the irrational number $\sqrt{d}$. An element a of this domain can be written as '$x+y\sqrt{d}$' with x and y two integers, so a is bijectively defined by $(x,y)\epsilon\mathbb{Z}^2$. We define $\overline{a}=x-y\sqrt{d}$ as the conjugate of a. Notice that $\overline{a}a=x^2-dy^2$. So (x,y) is a solution of the Pell equation if $\overline{a}a=1$ with $a=x+y\sqrt{d}$, in that case we know that $\overline{a}=a^{-1}$. Notice that for $a,b\epsilon\mathbb{Z}[\sqrt{d}]$ we have that $\overline{a}\overline{b}=(x-y\sqrt{d})(u-v\sqrt{d})=(xu+dyv)-(xv+yu)\sqrt{d}=\overline{ab}$. So if $\overline{a}a=1=\overline{b}b$ (they both represent a solution of the Pell equation), we have that $\overline{ab}ab=\overline{a}a\overline{b}b=1$ so we get another solution.

Notice that for $a\epsilon\mathbb{Z}[\sqrt{d}]$ with $a=x+y\sqrt{d}\geq 1$ and $\overline{a}a=1$ we have that $0<\overline{a}=a^{-1}\leq 1$. So we have $1/2\leq(1/2)(a+\overline{a})=x$ and $0\leq(1/2)(a-\overline{a})=y\sqrt{d}$, so $a\geq 1$ if and only if $x\geq 1$ and $y>0$. The converse is trivial. Notice that for any a with $\overline{a}a=1$, if $a=1$ then it is the trivial Pell solution and if $a>1$ then it gives a non-trivial solution.

Now consider two solution given by $1\leq a=x+y\sqrt{d}$ and $1\leq b=u+v\sqrt{d}$. Notice that $x^2-dy^2=1=u^2-dv^2$ means that $x<u\Leftrightarrow y<v$, so $1\leq a<b$ implies $x<u$ and $y<v$. So this means both coördinates x and y of the solutions are ordered the same way as the real values of $x+y\sqrt{d}$.

Because of this ordering, we can consider the smallest possible non-trivial solution, so the smallest $a\epsilon\mathbb{Z}[\sqrt{d}]$ such that $a>1$ and $\overline{a}a=1$. We know from the previous results that every power of a: a^n gives another solution of the Pell equation, and this solution is distinct for every n because $a>1$. Do these powers give all the positive solutions of the Pell equation? Consider a solution $b\epsilon\mathbb{Z}[\sqrt{d}]$ with $\overline{b}b=1$ and $1\leq b$. So b is a non-trivial positive solution of the equation. Obviously, there is an n such that $1\leq a^n\leq b<a^{n+1}$. So $1\leq ba^{-n}<a$, and we can see that $\overline{(ba^{-n})}ba^{-n}=\overline{(b)}a^n\overline{b(a^{-n})}=\overline{(b)}\overline{b}\overline{(a)}^n a^n=1$, so ba^{-n} gives another solution. But a was defined as the smallest non trivial solution, so ba^{-n} must be the trivial solution and must be equal to 1. So $b=a^n$. We can conclude that every non-negative solution of the Pell equation can be written as a power of this a.

Lemma, Solutions of the Pell equation: *(x,y) is a non-negative solution of the Pell equation if and only if there is an $n\epsilon\mathbb{Z}_{\geq 0}$ such that $x+y\sqrt{d}=(u+v\sqrt{d})^n$, were (u,v) is the smallest non-trivial positive solution of the Pell equation.*

Because of the ordering of solutions, there is a simple algorithm to find these (u,v). They are simply found by looking for the smallest $x>0$ for which $1+dx^2$ is a square, because then $(u,v)=(\sqrt{1+x^2d},x)$ is the smallest non-trivial solution.

5.2 Recursive properties of the solutions

We will now define (x_n) and (y_n) as the ascending row of non-negative solutions of the Pell equation, and we know that:

$$x_n+y_n\sqrt{d}=(u+v\sqrt{d})^n \tag{16}$$

From this we can derive a recursive formula by using the fact that $x_{n+1}+y_{n+1}\sqrt{d}=(u+\sqrt{d}v)^{n+1}=(u+v\sqrt{d})^n(u+v\sqrt{d})=(x_n+y_n\sqrt{d})(u+v\sqrt{d})=(x_nu+dy_nv)+(x_nv+y_nu)\sqrt{d}$, so we get:

$$x_{n+1}=x_nu+dy_nv \tag{17}$$

$$y_{n+1}=x_nv+y_nu \tag{18}$$

It is also relevant to look at more general addition rules. We know that $x_{n\pm m}+y_{n\pm m}\sqrt{d}=(x_n+y_n\sqrt{d})(x_m-y_m\sqrt{d})$, so we can see that:

$$x_{n\pm m}=x_ny_m\pm dy_ny_m \tag{19}$$

$$y_{n\pm m} = y_n x_m \pm x_n y_m \tag{20}$$

We can also find another formula by looking at $a = u + v\sqrt{d}$ again: $a^2 - 2ua + 1 = a^2 - (a+\overline{a})a + \overline{a}a = 0$, so $a^{n+2} - 2ua^{n+1} + a^n = 0$ where $a^k = x_k + y_k\sqrt{d}$, so:

$$x_{n+2} = 2ux_{n+1} - x_n \tag{21}$$

$$y_{n+2} = 2uy_{n+1} - y_n \tag{22}$$

Where the initial values of x are $x_0 = 1$ and $x_1 = u$, and the initial values of y are $y_0 = 0$ and $y_1 = v$. Also note that the x_n and y_n of a single solution does not have any prime factors in common, because looking at the Pell equation we can see that if something divides them both, it should divide 1 as well. So:

$$gcd(x_n, y_n) = 1 \tag{23}$$

Secondly, we see that the parity of the solutions stays the same after increasing the index by two, so: the parity of x_{2k} is the same as that for $x_0 = 1$ so it is odd, the parity of x_{2k+1} the same as for $x_1 = u$, for y_{2k} it is even because $y_0 = 0$ and for y_{2k+1} it is the same as for $y_1 = v$.
We can clearly see the exponential properties of the solutions with these relations, because $x_n u < x_{n+1} < 2ux_n$ and $y_n u < y_{n+1} < 2uy_n$, so:

$$uu^{n-1} < x_n < u(2u)^{n-1} \tag{24}$$

$$vu^{n-1} < y_n < v(2u)^{n-1} \tag{25}$$

In the next chapter, we will see how these inequalities help us get closer to the diophantine representation of arbitrary recursive enumerable sets.
Below, you can see a table of the first 10 solutions of the Pell equation for $d = 3$ and their exponential behavior as an example.

n	y_n	$log(y_n)$	$log(y_{n+1}/y_n)$
1	1	0	1.38629
2	4	0.38629	1.32176
3	15	2.70805	1.31730
4	56	4.02535	1.31698
5	209	5.34233	1.31696
6	780	6.65929	1.31696
7	2911	7.97625	1.31696
8	10864	9.29321	1.31696
9	40545	10.6102	1.31696
10	151316	11.9271	1.31696

6 The Julia Robinson prerequisites

In 1950, Julia Robinson presented a very useful result (in [4]), which was used to prove the DPRM-theorem. It demands a diophantine equation whose solutions should obey two properties, later to be called the Julia Robinson prerequisites. Because this proof does not lose single-foldness, it is also very handy to consider when trying to prove that exponentiation is single-fold diophantine. The theorem Julia Robinson proved goes as follows (the two parts between brackets should either both be ignored or both considered):

Julia Robinson prerequisites theorem $\{< a,b,c > | a = b^c\}$ *is (single-fold) diophantine if there is a Diophantine equation* $J(u,v,x_1,....,x_n) = 0$ *with unknowns* $u,v,x_1,...,x_n$ *(single-fold when* u *and* v *are taken to be arbitrary constants) with the following two properties:*
-$\forall k$ *there is a solution with* $v > u^k$
-In every solution $v < u^u$

Proof:
• Denote $(X_a(n), Y_a(n))$ as the n-th non-trivial solution of the Pell equation $x^2 - (a^2-1)y^2 = 1$. The first non-trivial solution is $(a,1)$, so we know that these solutions satisfy $X_a(n) + Y_a(n)\sqrt{a^2-1} = (a+\sqrt{a^2-1})^n$. Thus:

$$X_a(n) = \sum_{k=0,\ 2|k}^{n} \binom{n}{k} a^{n-k}(a^2-1)^{k/2}$$

We will write out two terms in detail, let b be an integer:

$$X_a(n)b^n = b^n \sum_{k=0,\ 2|k}^{n} \binom{n}{k} a^{n-k}(a^2-1)^{k/2} = \sum_{k=0,\ 2|k}^{n} \binom{n}{k} (ab)^{n-k}(a^2b^2-b^2)^{k/2}$$

$$X_{ab}(n) = \sum_{k=0,\ 2|k}^{n} \binom{n}{k} (ab)^{n-k}(a^2b^2-1)^{k/2}$$

Now assume $b > 1$, we can immediately see that $X_a(n)b^n \leq X_{ab}(n)$. On the other hand we have:

$$\frac{X_{ab}(n)}{X_a(n)b^n} = (\frac{a^2b^2-1}{a^2b^2-b^2})^{n/2} \leq (1-a^{-2})^{-n}$$

If we also assume $a > b^n$ we can now find that:

$$X_{ab}(n) \leq \frac{X_a(n)b^n}{(1-1/a^2)^n} < \frac{X_a(n)b^n}{1-n/a^2}$$

$$< \frac{X_a(n)b^n}{1-1/a} \leq \frac{X_a(n)b^n}{1-1/(b^n+1)} = X_a(n)(b^n+1)$$

So we see that with these two assumptions $b > 1$ and $a > b^n$ we have found that:

$$X_a(n)b^n \leq X_{ab}(n) < X_a(n)(b^n+1) \tag{26}$$

From this we can derive that:

$$(b > 1 \quad \& \quad a > b^n) \Rightarrow [c = b^z \Leftrightarrow X_a(n)c \leq X_{ab}(n) < X_a(n)(c+1)] \tag{27}$$

The converse $c = b^n \Rightarrow X_a(n)c \leq X_{ab}(n) < X_a(n)(c+1)$ is true because there can only be at most one c such that $X_a(n)c \leq X_{ab}(n) < X_a(n)(c+1)$, and because it is true for $c = b^n$ we get that indeed this is the case.

Let us again take $b > 1$ and $a > b^n$. We know that the sequence $(X_{ab}(n))_{n\epsilon\mathbb{N}}$ is an increasing sequence, so for $m < n$ we have:

$$X_{ab}(m) \leq X_{ab}(n-1) < X_a(n-1)(b^{n-1}+1) \leq X_a(n-1)a \leq X_a(n)$$

And for $m > n$ we have that:

$$X_{ab}(m) \geq X_{ab}(n+1) > abX_{ab}(n) > aX_a(n)$$

So we have found that $X_a(n) \leq X_{ab}(m) < X_a(n)a$ if and only if $m = n$.
So for a arbitrary integers u and n, if $u = X_{ab}(m)$ for some m and if $X_a(n) \leq u < aX_a(n)$, then we know for certain that $u = X_{ab}(n)$, so for all u, b, a and n we have:

$$(b > 1 \quad \& \quad a > b^n) \Rightarrow [u = X_{ab}(n) \Leftrightarrow [[\exists v : u^2 - (a^2b^2 - 1)v^2 = 1] \quad \& \quad [X_a(n) \leq u < aX_a(n)]]] \quad (28)$$

Combining the two results (27) and (28) we find that:

$$(1 < c < a \quad \& \quad b > 1 \quad \& \quad a > b^n) \quad (29)$$

$$\Rightarrow [c = b^n \Leftrightarrow (\exists u, v) : [(u^2 - (a^2b^2 - 1)v^2 = 1) \quad \& \quad X_a(n)c \leq u < X_a(n)(c + 1)]]$$

Before we continue, we define the diophantine relation:

$$\psi(a, u) := (\exists x, y) : [[x^2 - (a^2 - 1)((a - 1)y)^2 = 1] \quad \& \quad [x > 1] \ \& \ [a > 1] \ \& \ [u = ax]]$$

Recall from earlier results that $a^n \leq X_a(n) \leq (2a)^n$. We also know that if $\psi(a, u)$ is true, then there is an n such that $x = X_a(n)$ and $(a - 1)y = Y_a(n)$. So we know that:

$$Y_a(n) = \sum_{k=1, k \epsilon Odd}^{n} \binom{n}{k} a^{n-k}(a^2 - 1)^{(k-1)/2}$$

From which we can derive that $Y_a(n) \equiv na^{n-1} \bmod (a^2 - 1)$. So $n \equiv Y_a(n) = (a - 1)y \equiv 0 \bmod (a - 1)$.
So $n = (a - 1)k$ for some $k > 0$.
So we get $u = ax = aX_a(ak - k) \geq aX_a(a - 1) \geq aa^{a-1} = a^a$. So:

$$\psi(a, u) \Rightarrow u \geq a^a$$

We also know that if we take $u = aX_a(a - 1)$, then $\psi(a, u)$ is true and $u = aX_a(a - 1) \geq a^a$, so we get a second property of the relation:

$$(a > 1) \Rightarrow \exists_u(\psi(a, u) \quad \& \quad u \geq a^a)$$

With help of this newly found relation, we can replace the inequality $a > b^n$ with a stronger diophantine relation θ defined as:

$$\theta(a, b, n) := (\exists k, h) : [k > b \quad \& \quad k > n \quad \& \quad a > h \quad \& \quad \psi(h, k)] \Rightarrow (a > b^n)$$

Substituting this in (29) we get the relation for non trivial $c = b^n$ in terms of diophantine relations and Pell equations. We find that if $n > 1$ then $\forall c, b, n$:

$$c = b^n \Leftrightarrow [[b > 1] \quad \& \quad [c > 1] \quad \& \quad (30)$$

$$(\exists u, v, a) : [[c < a] \quad \& \quad [\theta(a, b, n)] \quad \& \quad [u^2 - (a^2y^2 - 1)v^2 = 1] \quad \& \quad [X_a(n)c \leq u < X_a(n)(c + 1)]]$$

Thus we can conclude that $c = b^n$ is diophantine in c, b and n, if $r = X_a(n)$ is diophantine in the parameters r, a and n.

• To finish of, we will now prove that if we have a diophantine equation as is in the assumption, then $r = X_a(n)$ is diophantine in r, a and n.
Let $\rho(u, v)$ be the relation satisfying the Julia Robinson prerequisites, so by the assumption in the

theorem it is diophantine. We can describe $r = X_a(n)$ in terms of this ρ and some other diophantine relations. Notice that:

$$[[1 < r < X_a(a)] \quad \& \quad [0 < z < a]] \Rightarrow [r = X_a(n) \Leftrightarrow \exists s : [r^2 - (a^2 - 1)(z + s(a - 1))^2 = 1]] \tag{31}$$

This because if $r^2 - (a^2 - 1)(z + s(a - 1))^2 = 1$ we know that there is an n such that $r = X_a(n)$ and $z + s(a - 1) = Y_a(n)$, so just like we did earlier we can derive that $z \equiv z + s(a - 1) \equiv n \bmod (a - 1)$. And because $z < a$ we get that $z = n$, so $r = X_a(n) = X_a(z)$.
Now, last but not least, notice that from the first JR prerequisite we know that if $r \leq d$ and $\rho(a, d)$ is true then $r \leq d < a^a < X_a(a)$. From the second JR prerequisite we know that for all a and n there is a d such that $d > X_a(n)$. So in conclusion:

$$(r = X_a(n)) \Leftrightarrow [[1 < r \leq d] \quad \& \quad \rho(a, d) \quad \& \quad [0 < z < a] \quad \& \quad \exists s : [r^2 - (a^2 - 1)(z + s(a - 1))^2 = 1]]$$

So we now know that $r = X_a(n)$ is diophantine in the parameters r, a and n if there exists a diophantine equation $J = 0$ satisfying the Julia Robinson prerequisites.
End of proof

□

We will now discuss what this theorem implies. Halfway through the previous proof, we have found that if $r = X_a(n)$ is diophantine in the parameters r, a and n, then we get that exponentiation is diophantine. But because of the theorem, we do not need to limit ourselves to the Pell equation. If we have a row (z_n) of which we know $a^n < z_n < b^n$, with $1 < a < b$, we can say that $\{< u, v > | v = z_u \quad \& \quad u > b\}$ satisfies the Julia Robinson properties. Because for every solution, $v = z_u < b^u < u^u$ and for every k it is obvious that we can find an u such that $v = z_u > a^u > u^k$, because the exponential formula goes faster than a constant power. So we can conclude:

Exponential row theorem *If a row of integers (z_n) with the property $Aa^n < z_n < Bb^n$ with $1 < a < b$ and $A > 0$ and $B > 0$ can be represented in a (single-fold/finite-fold) diophantine way, then exponentiation is (respectively single-fold/finite-fold) diophantine*

Proof: Define m as an integer such that $b^m > B$ and look at the relation $\{< u, v > | v = z_{u-m} \quad \& \quad u > m \quad \& \quad u > b\}$, then for every solution we have $v = z_{u-m} < Bb^{u-m} < b^m b^{u-m} = b^u < u^u$ so the second property is found. Because of the fact that exponentiation grows faster than a fixed power we can also say that for every k there is an u such that $v > z_{u-m} > Aa^{u-m} > u^k$. So both properties are met. Hence with the Julia Robinson theorem we can conclude that exponentiation is diophantine.

□

This is a really handy tool. We now know that if we have a diophantine row with exponential behavior we can prove that exponentiation is diophantine. The solutions of the Pell equation are an obvious contestant. The problem however is that with the equation alone, we can only find the an unordered set of solutions. We must find a way to link the solutions to its appropriate index. The next two chapters are about two attempts of doing so.

7 Proof of Martin Davis

This chapter is about the proof of Martin Davis ([7]). In this proof, Davis is forced to make a false assumption whereby his result could not be used. However, it is possible to weaken the assumption in

order to get the stronger result; exponentiation is single-fold diophantine.
This proof will show a direct method of finding the index of the solutions of the Pell equations by not looking at the whole row of solutions, but at a particular subrow: $(y_{2^n})_{n\epsilon\mathbb{N}}$. We will set d to 7, for reasons that will become clear later. For this d, we have that the initial solutions are $u = x_1 = 8$ and $v = y_1 = 3$. We will first see that if this subrow is diophantine, then we can prove that exponentiation is diophantine.

7.1 The sub-row to salvation

From our knowledge of the solutions of the Pell equation we can find the doublings-formula: $x_{2n} + y_{2n}\sqrt{7} = (8 + 3\sqrt{7})^{2n} = (x_n + y_n\sqrt{7})^2 = (x_n^2 + 7y_n^2) + (2x_n y_n)\sqrt{7}$. So:

$$x_{2n} = x_n^2 + 7y_n^2 \tag{32}$$

$$y_{2n} = 2x_n y_n \tag{33}$$

From this we can find that:

$$y_{2^n} = 2^n y_1 \prod_{k=0}^{n} x_{2^k} = 3(2)^{n+3} \prod_{k=1}^{n} x_{2^k} \tag{34}$$

Notice that y_{2n} is always even, so that means with $gcd(x_k, y_k) = 1$ that x_{2n} is always odd. So the only factors of 2 in y_{2n} is the power 2^{n+3}. This property is fundamental in the proof.

Let us assume for a moment that we are able to represent the set $\{y_{2^n}\}$ in a diophantine way (so $a = y_{2n}$ is diophantine in parameters a and n).
In section 7.2 and 7.3 we will prove that this assumption can be reduced to the Martin Davis' assumption.
The idea of this approach is to recognize the index x of y_{2^x} by means of the already diophantine relation $a \geq GPT(b)$, and knowing that $GPT(y_{2^x}) = 2^{x+3}$. Let us define the relation $\rho(m, n)$ as follows:

$$\rho(m, n) := [[\exists x : m = y_{2^x}] \quad \& \quad [n \geq 8GPT(m)] \quad \& \quad [n > 16]] \tag{35}$$

By our assumption and results from earlier chapters (for instance 14 from chapter 2), this is diophantine. Let us prove this relation satisfies the Julia Robinson Prerequisites:

Prerequisite I: Let $k > 0$, choose $n = 2^x$, where x is chosen such that $n > 16$ and $8^(n-1) > n^k$ (which is possible because you can always find an N such that $t > N$ implies $a^t > t^b$). Choose $m = y_n = y_{2^x}$. This is clearly an element of the diophantine relation, and we see that with (25) that $m = y_n > vu^{n-1} = 3(8)^{n-1} > n^k$. So that suffices for the first prerequisite.

Prerequisite II: For an element (m, n) of the relation, we know that there is an x such that $m = y_{2^x}$. Since $n \geq GPT(m) = 2^x$ and since the solutions of the Pell equation are strictly ascending, we have that $m = y_{2^x} \leq y_n \leq v(2u)^{n-1} = 3(16)^{n-1} < 3n^{n-1} < n^n$, because $n > 16$. So the second prerequisite is valid.

We can conclude that if we indeed have that $m = y_{2^n}$ is diophantine in m and n, then we know that exponentiation is diophantine.

7.2 The filter $x^2 + 7y^2$

So what does it take to prove that $m = y_{2^n}$ is diophantine in parameters m and n? To do this we will study when numbers that are represented in the form of $a^2 + 7b^2$, with a and b integers. Let us call the

set of numbers represented in this form K. It is better to talk about representability by x^2+7y^2 as being in elements of a set so we don't get confused with diophantine representability. So:

$$x \epsilon K \Leftrightarrow (\exists a, b) : [x = a^2 + 7b^2] \tag{36}$$

This is clearly a diophantine set. The information in this section is mostly from [16].
Firstly, if one has two numbers that are in K, say $x = a^2 + 7b^2$ and $y = c^2 + 7d^2$, you have that $xy = a^2c^2+7^2b^2d^2+7(a^2d^2+b^2c^2) = (a^2c^2-7abcd+7^2b^2d^2)+7(a^2d^2+abcd+b^2c^2) = (ac-7bd)^2+7(ad+bc)^2$. So its product is also in K. This is a result originally from Euler:

Lemma (Euler): *If m and n are in K, then mn is in K*

To further determine the elements of K, we must give some definitions. A prime p is called an essential prime of x^2+7y^2 if p is not 7, not 2 and there are x and y with $gcd(x, y) = 1$ (so also $y > 0$, very important) such that $p|(x^2 + 7y^2)$. Now we will prove the following lemma:

Essential prime lemma: *Let p be an odd prime, then p is an essential prime if and only if -7 is a square mod p and not equal to zero mod p.*

Proof:
Let p be an essential prime, then there are x and y such that $gcd(x, y) = 1$ and $p|(x^2 + 7y^2)$. So $x^2 \equiv -7y^2 \mod p$. We know that $y \not\equiv 0 \mod 7$ because else $x \equiv 0 \mod p$, so $p|gcd(x, y)$. So $-7 \equiv (xy^{-1})^2 \mod p$, so in other words a square modulus p.
Let -7 be a square mod p, then there is an x such that $-7 \equiv x^2 \mod p$. So $x \not\equiv 0 \mod p$. So there is a k such that $-7 = x^2 + kp$, or in other words $x^2 + 7(1)^2 = -kp$, thus p is an essential prime.

□

So by using calculations with quadratic residues, we can easily determine all essential primes of x^2+7y^2. The question now is, what combinations (products) of essential primes are elements of K.

To this extend we will look at two lemmas which will to help us get to the main result of this paragraph:

Lemma 7.1: *Let p be a prime and let s be an integer. Then there are x and y such that $p|(x^2 - s^2y^2)$ and $x^2 < p$ and $y^2 < p$ and x and y not both zero.*

Lemma 7.2: *If p and n are numbers with p or $-p$ a prime, pn in K and p in K, then n is in K*

With these lemma's, lets look what combinations of essential primes are possible. Notice that 7 is a prime in class 3 modulo 4. So the essential dividers of x^2+7y^2 are the primes p (not 2, not 7) such that $1 = \binom{-7}{p}$, -7 a square modulo p, which means $1 = \binom{-7}{p} = \binom{7}{p}(-1)^{(p-1)/2} = \binom{p}{7}(-1)^{(p-1)/2}(-1)^{(p-1)/2} = \binom{p}{7}$. So all primes which are not equal to 7 and 2, but which are quadratic modulo 7 are essential.
Let p be such a prime, then there is an s such that $s^2 \equiv -7 \mod p$. From Lemma 7.1 we have that there are x and y such that $(x, y) \neq (0, 0)$, $x^2 < p$, $y^2 < p$ and $p|(x^2 - s^2y^2)$. With the property that $p|(s^2 + 7)$ we get that $p|(x^2 + 7y^2)$ for these specific x and y. We know that $0 < (x^2 + 7y^2) < (1 + N)p$, so $k = (x^2 + 7y^2)\epsilon\{p, 2p, 3p, 4p, 5p, 6p, 7p\}$ Let us look at all possible values of k separately:

- If $k = p$, then p is representable.
- If $k = 7p$, then because 7 is representable, we get from Lemma 7.2 that p is representable.

• If $k = bp$ with $b < 7$ not a square mod 7 (so $b = 3$, $b = 5$ and $b = 6$), we get a contradiction because $x^2 + 7y^2$ is a square modulo 7 and p is a square modulo 7, so with lemma 7.2 we find that b is a square modulo 7.
• If $k = 2p$. Then either x and y are both odd or both even. If both even, then with $x = 2a$ and $y = 2b$, $4a^2 + 4(7b^2) = 2p$ which is impossible because p is odd. If both are odd, then $x = 2a + 1$ and $y = 2a + 1$, so $4a^2 + 4(7b^2) + 4a + 4(7b) + 1 + 7 = 2p$, so again $4|2p$ which is impossible. So $k \neq 2$.
• If $k = 4p$. Then either x and y are both zero or 1 mod 4. If both 0, then with $x = 4a$ and $y = 4b$, we get that $16a^2 + 16(7b^2) = 2p$ which is impossible because p is odd. If both are 1, then $x = 4a + 1$ and $y = 4a + 1$, so $16a^2 + 16(7b^2) + 8a + 8(7b) + 1 + 7 = 4p$, so again $8|4p$ which is impossible. So $k \neq 4$.

We can conclude that for all possible k our result means that p is representable, so p is representable. So all essential primes of $x^2 + 7y^2$ are representable.

Of course we know that all squares are also in K, because we can take $x^2 + 7(0^2) = x^2$. And if for $k = x^2 + 7y^2$ we have that $gcd(x, y) = a \neq 1$, then $a^2|k$. So we have that any product of essential primes and squares are elements of K. By definition of essential primes, no other combination of factors can be used. So we can say:

K representability theorem *An integer a is an element of K if and only if $a = b^2 p_1 ... p_n$ with $p_1, .., p_n$ primes which are squares modulo 7 (so equivalent to 1,2 or 4 modulo 7).*

7.3 Elements filtered

How is the knowledge of the previous section going to help us? In this section we will prove that $m = y_{2^n}$ is diophantine in m and n if we assume that the Martin Davis equation only has the trivial solution.
We can easily see with the fact that $4 = (2)^2 + 7(0)^2$ and $8 = (1)^2 + 7(1)^2$ that all 2^m with $m \geq 2$ are elements of K. Also, from (32) we have that $x_{2n} = x_n^2 + 7y_n^2$, so one can say that $(y_{2^n}/3) = 2^{n+3} \prod_{k=1}^{k=n} x_{2^k}$ is in K.

Now we want to prove that if $y_n/3$ is not in K, if n is not an power of 2. Before we continue, notice that we can always divide by 3 because $y_0 = 0$ and $y_1 = 3$ are divisible by 3, so by (22) all y_n are.

Let us call all odd primes not 7 which are not squares modulo 7 non-essential primes. Then from the results of the previous section any power of essential primes are allowed and only even powers of non-essential primes are allowed.
So we can say that if an x contains an odd power of a certain non-essential prime, it is not in K.
Also, if x is odd and it is not in K, then it must have an odd power of a certain non-essential prime.
We will now prove that y_m is not in K if there is no n such that $m = 2^n$ and we assume that $9(u^2 + 7r^2)^2 - 7(r^2 + 7s^2)^2 = 2$ only has the trivial solution. We will do this by using two inductive steps.

Step I: *Say n is even but not a power of 2, so there are $m > 0$ and $k > 2$ such that $n = 2^m k$. Then we have that $y_k/3$ is in K only if $y_n/3$ is in K.*

Proof:
Assume $y_k/3$ is not in K. We know by definition that k is odd, and because of parity properties we get that y_k is odd. So $y_k/3$ must contain an odd power of a certain non-essential prime, let's call that prime p. Using (33) we can find that: $y_{2^m k}/3 = 2^m (y_k/3) x_k \prod_{h=1}^{h=n} x_{2^h k}$. Remember that $3|y_k$. By (32)

we know that any $x_{2^h k}$ with $h \geq 1$ is representable, so if they contain p, they must have him to an even power. Also, p is odd so it does not divide 2^m. Because p divides y_k and $gcd(x_k, y_k) = 1$, we also have that p does not divide x_k. So because $y_k/3$ has p to an odd power and all other elements of $y_{2^m k}/3$ have p to an even power, we can conclude that $y_{2^m k}/3$ has an odd power of p, and because p was non-essential we can conclude that $y_{2^m k}/3$ is not in K.

□

Step II: *Say n is odd, so there is a k such that $n = 2k + 1$. If $y_{2k+1}/3$ is in K, then both $x_k + 7(y_k/3)$ and $x_k + 3y_k$ should be in K.*

Proof:
We know that $x_{2k+1} + y_{2k+1}\sqrt{7} = (x_k + y_k\sqrt{7})^2(x_1 + y_1\sqrt{7}) = ((x_k^2 + 7y_k^2) + 2x_k y_k\sqrt{7})(8 + 3\sqrt{7})$ so $y_{2k+1} = 3x_k^2 + 16x_k y_k + 21y_k^2 = (3x_k + 7y_k)(x_k + 3y_k) = (x_k + 7(y_k/3))(x_k + 3y_k)$. Define d such that $d|(x_k + 7(y_k/3))$ and $d|(x_k + 3y_k)$. We know that d is odd because $(x_k + 3y_k)$ is odd ($gcd(x_k, y_k) = 1$). Also, $d|(3(x_k + 3y_k) - 3(x_k + 7(y_k/3))) = 2y_k$, so $d|y_k$. This means that $d|((x_k + 3y_k) - 3y_k) = x_k$. But again $gcd(x_k, y_k) = 1$, so $d = 1$. We can conclude that $gcd(x_k + 7(y_k/3), x_k + 3y_k) = 1$. So if either $x_k + 7(y_k/3)$ or $x_k + 3y_k$ is not in K, then one of them must contain an odd power of a non-essential prime p and the other does not contain that prime. So $y_{2k+1}/3$ has an odd power of that non-essential prime and is not in K.

□

These two steps inductively lead to the following fact, if $x_k + 7(y_k/3)$ and $x_k + 3y_k$ are never in K for any k, we can conclude with induction that for all n not a power of 2, y_n is not in K.

So what does it mean if $x_k + 7(y_k/3)$ and $x_k + 3y_k$ is in K. It means that for a solution of the Pell equation $x_n^2 - 7y_n^2 = 1$ there are u, v, r and s such that $x_k + 7(y_k/3) = u^2 + 7v^2$ and $x_k + 3y_k = r^2 + 7s^2$. Taking $X = x_n$ and $Y = y_n/3$, for which we have:
$2 = 2(x_n^2 - 7y_n^2) = 2(X^2 - 7(3Y)^2) = 2(X^2 - 63Y^2) = (9 - 7)X^2 + (441 - 567)Y^2 + (126 - 126)XY = 9(X^2 + 14XY + 49Y^2) - 7(X^2 + 18XY + 81Y^2) = 9(X + 7Y)^2 - 7(X + 9Y)^2 = 9(u^2 + 7v^2)^2 - 7(r^2 + 7s^2)^2$ so we get (3).

$$9(u^2 + 7v^2)^2 - 7(r^2 + 7s^2)^2 = 2$$

So if y_n is in K and n is not an power of 2, we have that (3) has a non-trivial solution. Reversing that statement, one can say that if (3) does not have any non-trivial solutions, y_n can never be in K if n is a power of 2. So one would get y_n is in K if and only if n is a power of two, resulting in the diophantine representation of $m = y_{2^x}$ in the parameters m and x:

$$\exists x : [b = y_{2^x}] \Leftrightarrow (\exists a, t, f) : [a^2 - 7b^2 = 1 \quad \& \quad b = t^2 + 7f^2] \tag{37}$$

Unfortunately, many non-trivial solutions of (3) have been found since Martin's original publication of this proof. But there is hope yet, if one can prove that there are only a finite number of solutions of this equation, one can for instance create the finite set $W = \{(3(u^2+7v^2))|(\exists r, s)[9(u^2+7v^2)^2 - 7(r^2+7s^2)^2 = 2]\}$. When using (8) on every element of W, one can represent in a diophantine way the relation of not being in the set W. If a solution of the Pell equation is in K, and does not coincide with one of the solutions of (3) one knows that its index is a power of 2. This would give the diophantine representation:

$$\exists x : [b = y_{2^x}] \Leftrightarrow (\exists a, t, f) : [a^2 - 7b^2 = 1 \quad \& \quad b = t^2 + 7f^2 \quad \& \quad (3a - 7b)\epsilon(\mathbb{N} - W)] \tag{38}$$

This representation is by construction finite-fold, because there are only a finite number of t and f such that $b = t^2 + 7f^2$ and one a such that $a^2 - 7b^2 = 1$. So we can conclude with the following theorem:

Salvaged Martin Davis Theorem *If* $9(u^2+7v^2)^2-7(r^2+7s^2)^2=2$ *only has a finite number of solutions then any recursively enumerable relation is finite-fold diophantine*

As an overview, here is the structure of the proof in short: If (3) only has a finite number of solutions, then the row $m=y_{2^n}$ is finite-fold diophantine in m and n, which gives us a diophantine equation which satisfies the Julia Robinson prerequisites in a finite way, from which we can conclude that exponentiation is finite-fold diophantine, which closes the gap of the proof that r.e. relations are finite-fold diophantine.
Let us hope that this weakened assumption is true.

8 Matiyasevich proof of the DPRM-theorem

Now for the successful attempt of proving that exponentiation is diophantine, originally published in [8] and later in the book [14]. Because it uses a lot of calculations in modulo equivalence, this proof does not show that exponentiation is single-fold diophantine, only that it is diophantine. For this proof we look at an arbitrary d in the form of $d=a^2-1$, with $a\geq 1$. We will define $(X_a(n),Y_a(n))$ as the row of solutions for a fixed a. We know that the lowest non-trivial solution of this Pell equation is $(x_a(1),y_a(1))=(a,1)$, so the solutions of the Pell equation $x^2-(a^2-1)y^2=1$ can be define the solutions in the following two equivalent ways as discussed before in the Lemma and (21):

(X_a,Y_a) is a solution if and only if there is an $n\epsilon\mathbb{Z}_{\geq 0}$ such that $X_a+Y_a\sqrt{d}=(u+v\sqrt{d})^n=(a+\sqrt{a^2-1})^n$

Let us define the recursive row $X_a(0)=1$, $X_a(1)=a$, $X_a(n+2)=2aX_a(n+1)-X_a(n)$ and $Y_a(0)=0$, $Y_a(1)=1$, $Y_a(n+2)=2aY_a(n+1)-Y_a(n)$. We know that this row gives us all the solutions of the Pell equation with $d=a^1-a$.

8.1 Congruence properties

First note that $Y_a(n)$ is polynomial in a, which you can conclude from the recursive definition. From this we can derive that $b=a$ is a zero of the polynomial $F(b)=Y_a(n)-Y_b(n)$ with unknown b, so we can state the *congruence rule*:

$$(a-b)\mid(Y_a(n)-Y_b(n)) \tag{39}$$

In particular, we know from our recursive property that $Y_1(n)=n$, so we also know that:

$$Y_a(n)\equiv n \mod (a-1) \tag{40}$$

Lemma 8.1: $n|m$ *if and only if* $Y_a(n)|Y_a(m)$

Proof: We know from (19) that $Y_a(k\pm n)=Y_a(k)X_a(n)\pm X_a(k)Y_a(n)\equiv Y_a(k)X_a(n)$ modulo $Y_a(n)$. With gcd($X_a(n)$,$Y_a(n)$) = 1 we can see that $Y_a(n)|Y_a(k\pm n)$ if and only if $Y_a(n)|Y_a(k)$. Because trivially $Y_a(n)|Y_a(n)$, so we can conclude by repeatedly using this rule that k must be a multiple of n if and only if $Y_a(n)|Y_a(k)$.

□

Lemma 8.2: $Y_a^2(n)|Y_a(m)$ *if and only if* $(nY_a(n))|m$

Proof: We know that $X_a(nk) + Y_a(nk)\sqrt{d} = (X_a(n) + Y_a(n)\sqrt{d})^k$, so $Y_a(nk) = \sum_{i=0}^{(k-1)/2} \binom{k}{2i+1} X_a(n)^{k-2i-1} Y_a(n)^{2i+1} d^i$. So:

$$Y_a(nk) \equiv kX_a(n)^{k-1} Y_a(n) \mod Y_a(n)^3 \tag{41}$$

Assume $(nY_a(n))|m$. Choose $k = Y_a(n)$, then we know from (41) that $Y_a(n)^2|Y_a(nY_a(n))$, so with lemma 8.1 we get that $Y_a(n)^2|Y_a(m)$.
Assume $Y_a(n)^2|Y_a(m)$, then with lemma 8.1 we have that $n|m$, say $m = nk$. From the previous result (41) and $gcd(X_a(n), Y_a(n)) = 0$ that $Y_a(n)^2|kY_a(n)$. So $Y_a(n)|k$, so $(nY_a(n))|m$.

□

That concludes the proof of lemma 8.2. Let us now derive a helpful relation for the last lemma.

Note that from the doublings-formulas (33) and (32) we have that $Y_a(2n) \equiv 0 \mod X_a(n)$ and $X_a(2n) \equiv -1 \mod X_a(n)$. Using this combined with the addition rules in (19) we get that $Y_a(2n \pm m) \equiv \mp Y_a(m) \mod X_a(n)$. So using that twice we get $Y_a(2n + (2n \pm m)) \equiv \pm Y_a(m) \mod X_a(n)$. Using it an arbitrary amount of times we get that for all natural numbers i, n and m:

$$Y_a(4ni \pm m) \equiv Y_a(m) (mod(X_a(n))) \tag{42}$$

$$Y_a(4ni + 2n \pm m) \equiv \mp Y_a(m) (mod(X_a(n))) \tag{43}$$

With help of these relations (we will call them the $4n$-relations) we can find the final lemma:

Lemma 8.3: *$Y_a(k) \equiv \pm Y_a(m)$ (mod $(X_a(n))$) if and only if either $k \equiv m$ (mod $2n$) or $k \equiv -m$ (mod $2n$).*

Proof: Take $a \leq 2$ and $1 \leq n$.
Assume $k \equiv \pm m$ (mod 2n), take $k = 2nj \pm m$. We can immediately conclude from the $4n$-relations (looking at $j = 2i$ and $j = 2i + 1$ separately) that indeed either $Y_a(k) \equiv Y_a(m)$ (mod $(X_a(n))$) or $Y_a(k) \equiv -Y_a(m)$ (mod $(X_a(n))$).

Assume $Y_a(k) \equiv \pm Y_a(m)$ (mod $(X_a(n))$). Let h be defined such that $h \equiv \pm k$ mod $(2n)$ and $0 \leq h \leq n$. Define l such that $l \equiv \pm m$ mod $(2n)$ and $0 \leq l \leq n$. So from what we already have proven in this lemma, we can see that $Y_a(k) \equiv \pm Y_a(h)$ (mod $(X_a(n))$) and $Y_a(l) \equiv \pm Y_a(m)$ (mod $(X_a(n))$), so with our assumption we have $Y_a(h) \equiv \pm Y_a(l)$ (mod $(X_a(n))$). So $X_a(n)|(Y_a(h) \pm Y_a(l))$.
If $h \neq l$, we have that $0 < |Y_a(h) \pm Y_a(l)| \leq |Y_a(h) + Y_a(l)| \leq Y_a(n-1) + Y_a(n)$. We know that in the solutions of the Pell equation, $X_a(n) > Y_a(n)$, so $|Y_a(h) \pm Y_a(l)| < Y_a(n-1) + Y_a(n) < X_a(n)$, which is not possible if $X_a(n)|(Y_a(h) \pm Y_a(l))$, contradiction.
So $h = l$. We can deduce from this that $h \equiv \pm l$ mod $(2n)$, so also $k \equiv \pm m$ mod $(2n)$.
This concludes the proof of Lemma 8.3 .

□

8.2 System of equations

Now we have all the needed lemmas about congruence relations out of the way, we can finally look at a specific diophantine system of the relation $C = Y_A(B)$ with parameters A, B and C.
We will look at the next system of Diophantine equations/relations with unknowns D, E, F, G, H, I:

(I): $D^2 - (A^2 - 1)C^2 = 1$

(II): $F^2 - (A^2 - 1)E^2 = 1$
(III): $I^2 - (G^2 - 1)H^2 = 1$
(IV): $2C^2|E$
(V): $G \equiv A \pmod{F}$
(VI): $G \equiv 1 \pmod{2C}$
(VII): $H \equiv C \pmod{F}$
(VIII): $H \equiv B \pmod{2C}$
(IX): $B \leq C$

With the previous congruence results we can prove that for $A > 1$ this system has a solution if and only if $C = Y_A(B)$.

Proof:
• Let us take a solution of this system with $A > 1$, so $A, B, C, D, E, F, G, H, I$ obey the equations (I-IX). The first three equations (I-III) are all Pell equations in the form of what we have studied this chapter. So we can find p, q and r such that $D = X_A(p)$, $C = Y_A(p)$, $F = X_A(q)$, $E = Y_A(q)$, $I = X_G(r)$ and $H = Y_G(r)$. We want to prove that $B = p$.
From (IV) we know that $C^2|E$, so $Y_A(p)^2|Y_A(q)$. With lemma 8.2 we then know that $Y_A(p)|q$, so $C|q$.
From (VI) we know that $2C|(G-1)$, so with (40) we get that $H = Y_G(r) \equiv r \bmod 2C$. So with (VIII) we get that $B \equiv r \bmod 2C$.
From (V) we know that $F|(A-G)$, so with (39) we get $Y_A(r) \equiv Y_G(r) \bmod X_a(q) = F$. (VII) says $H \equiv C \pmod{F}$, so $Y_A(r) \equiv Y_A(p) \bmod F$. This together with Lemma 8.3 means $r \equiv \pm p \bmod 2q$.
So we know $C|q$, $B \equiv r \bmod 2C$ and $r \equiv \pm p \bmod 2q$. We can conclude that $B \equiv \pm p \bmod 2C$. We know that in general $0 \leq n \leq Y_a(n)$, so $0 \leq p \leq C$. With (IX) we have that for B we also have $0 \leq B \leq C$. So $B = p$,
Conclusion: $C = Y_A(B)$.

• Now for the converse, let us take A, B and C such that $C = Y_A(B)$. We want to prove that there are D, E, F, G, H, I which obey (I-IX).
Notice (IX) already holds. Take $D = X_A(B)$, we see that the first Pell equation in (I) holds.
Define $q = BY_A(B)$ and take $F = X_A(2q)$ and $E = Y_A(2q)$ so the $2q$-th solution of (II).
From lemma 8.2 we know that $C^2 = Y_A(B)^2|Y_A(BY_A(B)) = Y_A(q)$. The doubling formula in (33) implies $2C^2 = (2X_A(q)Y_A(q))|Y_A(2q) = E$. So (IV) holds.
Choose $G = A + F^2(F^2 - A)$, so (V) holds. From (II and IV) we know that $2C|(F^2 - 1)$, so (VI) holds as well.
Choose $I = X_G(B)$ and $H = Y_G(B)$ which give a solution of (III). With the congruence rule in (40) we know that $H \equiv B \bmod (G-1)$. With (VI) this means (VIII) holds.
With the general congruence rule (39) we know that $H \equiv C \bmod$ (G-A). With (V) we have that (VII) holds.

□

That concludes the proof. So we now know that the relation $C = Y_A(B)$ with parameters A, B and C is diophantine. Combining this result with the theorem of Julia Robinson, we get that exponentiation is diophantine. Thus we now have proven the DPRM theorem:

DPRM theorem: *Every recursively enumerable relation is diophantine*

9 A universal diophantine equation

This chapter will be an intermission about a special type of diophantine equation, a universal one.
A universal diophantine equation is an equation that is able to generate all possible diophantine sets of a certain rank. Formally, if we take an arbitrary $n > 0$, then the universal diophantine equation with rank n is a diophantine equation $U(a_1, a_2, ..., a_n, k, x_1, x_2, ..., x_r) = 0$ with unknowns $a_1, a_2, ..., a_n, k, x_1, x_2, ..., x_r$ such that:
For any diophantine set $A \epsilon \mathbb{N}^n$ there is a k such that $(a_1, a_2, ..., a_n) \epsilon A \Leftrightarrow \exists x_1, \exists x_2, ..., \exists x_r : U(a_1, a_2, ..., a_n, k, x_1, x_2, ..., x_r) = 0$.
In this chapter, we will prove its existence using some newly introduced tools and using some old ones.

9.1 The Cantor ordering

Cantor gave a bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$ given by the function $Cantor(a, b) = \frac{(a+b)^2+3a+b}{2}$. Luckily for us, this function is almost diophantine, we just have to multiply both sides by two. So both coördinates are also diophantine, we can define the following two diophantine relation;
The relation $CantorA(c) = a$ in parameters a and c will be defined as: there is a b such that $2c = 2Cantor(a, b)$
And the relation $CantorB(c) = b$ in parameters b and c as: there is an a such that $2c = 2Cantor(a, b)$.

By induction we can find a bijection between $\mathbb{N}^n$ and $\mathbb{N}$, define $Cantor_1(a_1) = a_1$ and $Cantor_n(a_1, ..., a_n) = Cantor_{n-1}(a_1, ..., a_{n-2}, Cantor(a_{n-1}, a_n))$ for $n > 1$.
Again, this can be made diophantine for fixed n by multiplying both sides by 2^{2^n} and this way we can also define the diophantine relation $x = CantorE_{m,n}(c)$, as the m-th coördinate of an element $x \epsilon \mathbb{N}^n$ for which $c = Cantor_n(x)$. This relation is diophantine in parameters x and c for fixed m and n.

So $CantorE_{m,n}(c) = a_m$ is diophantine in the parameters c and a_m for fixed m and n. But we will want to find some diophantine way to order elements of arbitrary dimension (in $\mathbb{N}^n$ for arbitrary n). Let $n > 0$ and take an arbitrary element $(a_1, ..., a_n)$ of $\mathbb{N}^n$. Define $b = max(n, a_1, ..., a_n)!$, and then take $b_1, ..., b_n$ to be $b_i = bi + 1$ for all $i = 1, ..., n$.
Notice that all b_i are pairwise relative prime; if for some i and j there is a d such that $d|b_i$ and $d|b_j$, then $d|(b(i - j))$, so either $d|b$ or $d|(i - j)$, the latter also implies $d|b$ because $|i - j| < n$ and $n!|b$. So $d|b$ and $d|(bi + 1)$, so $d = 1$.
Secondly, notice that $a_i < b_i$ for all $i = 1, ..., n$. $b_i = bi + 1 > b \geq max(n, a_1, ..., a_n) \geq a_i$.
Now, using the *Chinese remainder theorem*, define a such that a_i is the remainder of dividing a by b_i.
So we have two numbers, a and b, from those we can create all the coördinates of $(a_1, ..., a_n)$ in a diophantine way; take $i = 1, ..., n$, then $a_i = rem(a, (bi+1))$. Let us call $CantorG(a, b, i) = rem(a, (bi+1)) = a_i$.
We now know that (a, b, n) where a and b as before and n the dimension gives us a diophantine description of $(a_1, ..., a_n)$, meaning that we can deduce $(a_1, ..., a_n)$ from (a, b, n) in a diophantine way.

9.2 Universal

A diophantine equation is just an integral polynomial equated to zero. When looking at a diophantine equation with non-negative unknowns, it is possible to split the polynomial in two and construct some polynomials $P(x_1, ..., x_n)$ and $Q(x_1, ..., x_n)$ with only non-negative coefficients such that $P(x_1, ..., x_n) = Q(x_1, ..., x_n)$ yields the same solutions as the old equation. This can be done by working out the brackets and transport all parts with a negative coefficient to the other side of the equation.
This is handy because there is a recursive way to define all natural polynomials (where unknowns and coefficients are non-negative), using the definition discussed in the Introduction:

• For all $k \epsilon \mathbb{N}$, k itself is a natural polynomial.
• For any unknown x_n, x_n itself is a natural polynomial.
• If P and Q are natural polynomials, then $P + Q$ is a natural polynomial.
• If P and Q are natural polynomials, then PQ is a natural polynomial.

These rules give us all the possible natural polynomials. With help of the Cantor-function, we can now sort all these possible equations by putting them in one recursive row $\{P_n\}_{n \epsilon \mathbb{N}}$. Define for all $k > 0$, $P_{4k} = k$ and $P_{4k+3} = x_{k+1}$, so we now have all numbers and unknowns in the sequence. Using Cantors function, we can find i and j such that $Cantor(i, j) = k$. So we can now define $P_{4k+1} = P_i + P_j$ and $P_{4k+2} = P_i P_j$. Because of the nature of Cantors function, we know that all possible natural values of i and j are used, so any summation and multiplication of two arbitrary elements already in the sequence is also later on in the sequence. So this sequence contains all natural polynomials.

Now take an a collection of natural numbers $p_0, p_1, ..., p_{r-1}$. We say that this collection is a realization of the sequence of polynomials if there are some $x_1, x_2, x_3, ...$ such that $p_i = P_i(x_1, x_2, x_3, ...)$. With the method in the previous section we can represent this equation in a diophantine way by the numbers p, q and r, such that $CantorG(p, q, i + 1) = p_i$ for all $i = 0, 1, ..., r - 1$.
We can use the fact that the $CantorG$ function is diophantine to find p and q such that $p_0 = CantorG(p, q, 1)$, $p_1 = CantorG(p, q, 2)$, ..., $p_{r-1} = CantorG(p, q, r)$. In other words, we can find p, q such that there are $x_1, x_2, ...$ for which $P_i(x_1, x_2, ...) = CantorG(p, q, i + 1)$ for all $i = 0, 1, ..., r - 1$ in a diophantine way.
And by definition of the polynomial sequence, we know that for k, i and j where $k = Cantor(i, j)$; $p_{4k} = k$, $p_{4k+1} = p_i + p_j$, $p_{4k+2} = p_i p_j$ and p_{4k+3} can be anything because of the free choice of the unknown x_{k+1}. It is not hard to see that if a sequence $p_0, p_1, ..., p_r$ satisfies those conditions, then there are $x_1, x_2, ...$ such that $p_i = P_i(x_1, x_2, ...)$ for all $i = 0, 1, ..., r - 1$.

So (p, q, r) is a code of the realization of the polynomial sequence if and only if:

For all $l < r$ we have that there are i, j, k with $Cantor(i, j) = k$ and $4k \leq l < 4(k + 1)$ such that:
• If $l = 4k$ then $k = CantorG(p, q, l + 1)$, $(p_{4k} = k)$.
• If $l = 4k + 1$ then $CantorG(p, q, l + 1) = CantorG(p, q, i + 1) + CantorG(p, q, j + 1)$, $(p_{4k+1} = p_i + p_j)$
• If $l = 4k + 2$ then $CantorG(p, q, l + 1) = CantorG(p, q, i + 1)CantorG(p, q, j + 1)$, $(p_{4k+1} = p_i p_j)$.

We will call this relation $PolynSeq(p, q, r)$. Notice that this relation is almost diophantine, safe from one bounded universal quantifier $\forall l < r$. Notice that i, j, k are all smaller than l, so also smaller than r. So our universal quantifier is bounded by the same number as existential quantifiers in this statement. So this predicate is of the form as in the Martin Davis Theorem in chapter 4, of which we proved in Lemma 4.5 that those types of predicates are diophantine. So we can conclude that $PolynSeq(p, q, r)$ is diophantine.

Now, let us take an arbitrary diophantine set $A \subset \mathbb{N}^n$. So there is an integral polynomial $D(a_1, a_2, ..., a_n, x_{n+1}, ..., x_m)$ such that $D(a_1, a_2, ..., a_n, x_{n+1}, ..., x_m) = 0$ represents the set. So there must be two natural polynomials P and Q such that $P(a_1, a_2, ..., a_n, x_{n+1}, ..., x_m) = Q(a_1, a_2, ..., a_n, x_{n+1}, ..., x_m)$ also represents A, so there must be i and j such that $P_i(a_1, a_2, ..., a_n, x_{n+1}, x_{n+2}, ...) = P_j(a_1, a_2, ..., a_n, x_{n+1}, x_{n+2}, ...)$ also represents A. So we can say that this equation is the number $k = Cantor(i, j)$ diophantine equation, and its solution space is the number k diophantine space. Any diophantine set is a projection of a solution space, so for any

diophantine set there must be a k and an n such that A is the projection of the number k diophantine solution space in the first n coördinates.

Now take an arbitrary k and n, and let A be the diophantine set which is the n-dimensional projection of the number k diophantine solution space.
Take an arbitrary collection of numbers $a_1, a_2, ..., a_n$. We know that $(a_1, ..., a_n)\epsilon A$ if and only if there are $x_1, x_2, ...$ such that $P_i(a_1, a_2, ..., a_n, x_{n+1}, x_{n+2}, ...) = P_j(a_1, a_2, ..., a_n, x_{n+1}, x_{n+2}, ...)$. So:

$$(a_1, ..., a_n)\epsilon A \Leftrightarrow$$

$$\exists i, j, p, q, r[[k = Cantor(i, j)] \quad \& \quad [r > i] \quad \& \quad [r > j] \quad \& \quad PolynSeq(p, q, r)$$

$$\& \ [CantorG(p, q, i + 1) = CanorG(p, q, j + 1)] \ \& \ [CantorG(p, q, 4) = a_1 \ \&...\& \ CantorG(p, q, 4n) = a_n]]$$

Notice what happens. This statement finds the i and j belonging to k and the three p, q, r which not only are a realization of the polynomial sequence, but also have the added quality that $p_i = p_j$, so it gives any solution of $P_i = P_j$. Then it selects the first n unknowns by using the fact that $P_{4h+3} = x_{h+1}$. This statement is clearly diophantine in the parameters $a_1, a_2, ..., a_n$ and k. So this whole statement is a diophantine representation of the universal diophantine set.
We can conclude that the universal diophantine equation exists.

10 Single-fold DPR-theorem

We will now look at the proof that all recursive enumerable sets are single-fold exponential diophantine. This proof was originally published in [10]. For single-fold we need to refine some stuff, we want to change everything in the original proof in such a way that they become single-fold. First note that we now already know that all recursively enumerable sets are diophantine, so we can use this for this proof.

10.1 Single-fold theorems

Firstly, remember the Cantor ordering from the previous chapter. For each n, we have an integer polynomial: $I_n(a_1, ..., an) := Cantor_n(a_1, ..., a_n)$ which orders the elements of $\mathbb{N}^n$ in the following way: $(a_1, ..., a_n)\epsilon\mathbb{N}^n$ goes after $(b_1, ..., b_n)\epsilon\mathbb{N}^n$ if and only if $I_n(a_1, ..., a_n) > I_n(b_1, ..., b_n)$. Not only that, for all integers $y > 0$ there is exactly one element $(a_1, ..., a_n)\epsilon\mathbb{N}^n$ such that $I_n(a_1, ..., a_n) = y$, so it gives us a neat single-fold diophantine ordering.
Also remember that $I_n = Cantor_n$ contains rational non-integer coefficients, but $2^{2^n} I_n$ does not. So $2^{2^n} I_n(a_1, ..., a_n) = 2^{2^n} y$ is diophantine in $y, a_1, ..., a_n$.
Now we need to improve the theorem that started it all by using the fact that we know that a recursively enumerable set already has a diophantine equation. We can write our r.e. relation in three other arithmetic ways:

Single-fold Davis Theorem: *For every recursively enumerable relation $R(a_1, ..., a_n)$ there are polynomials $E(a_1, ..., a_n, x)$ with unknowns $a_1, ..., a_n, x$ and $D(x, y, u_1, ..., u_m)$ with unknowns $x, y, u_1, ..., u_m$, both with non-negative coefficients such that the following statements are equivalent:*

$$R(a_1, ..., a_n) \Leftrightarrow$$

$$(\exists x)(\forall y \leq x)(\exists u_1, ..., u_m \leq E(a_1, ..., a_n, x)) : [D(a_1, ..., a_n, x, y, u_1, ..., u_m) = 0] \Leftrightarrow$$

$$(\exists! x)(\forall y \leq x)(\exists u_1, ..., u_m) : [D(a_1, ..., a_n, x, y, u_1, ..., u_m) = 0] \Leftrightarrow$$

$$(\exists x)(\forall y \leq x)(\exists! u_1, ..., u_m) : [D(a_1, ..., a_n, x, y, u_1, ..., u_m) = 0]$$

Because of the diophantine bijective map between $\mathbb{N}^n$ and $\mathbb{N}$, we will only prove this for $n = 1$.

Proof:
Let $P(a)$ be an enumerable predicate (So there is a set $A \subset \mathbb{N}$ such that $P(a) \Leftrightarrow a \epsilon S$) and let us take $M(a, z_1, ..., z_m) = 0$ as a diophantine representation of this enumerable predicate. Now we are going to use the Cantor ordering. For a certain value of a, if it satisfies the predicate, we know that $M = 0$ has solutions in $(u_1, ..., u_m)$. With the Cantor ordering we can give an unique value to this set of m integers, we can find the minimal value of all possible solutions. For all sets of m-tuples with a lower value, $M(a, z_1, ..., z_m)$ will not be zero. So we can say that:

$$P(a) \Leftrightarrow (\exists x)(\forall y \leq x)(\exists u_1, ..., u_m) : [y = I_m(u_1, ..., u_m) \quad \& \quad [[y < x \quad \& \quad M(a, u_1, ..., u_m) \neq 0] \quad (44)$$
$$OR \quad [y = x \quad \& \quad M(a, u_1, ..., u_m) = 0]]]$$

Notice that $u_1, ..., u_m$ are fully determined by $y = I_m(u_1, ..., u_m)$. This relation is basically saying that only the set of numbers belonging to $y = x$ should be a solution of $M = 0$, and any set belonging to a value lower than x should not be a solution of $M = 0$. So we force x to be the value belonging to the minimal solution of $M = 0$.
So we see that the right hand side is fully single-fold diophantine. So this gives us the polynomial D needed in the theorem. If you want something more specific, here is an example of the polynomial $D(a, x, y, u_1, ..., u_m)$ as the representation of (44):

$$2^{2^m}(y - I_m(u_1, ..., u_m))^2 + ((x - y)M^2(a, u_1, ..., u_m) - 1 - u_0)^2((x - y)^2 + M^2(a, u_1, ..., u_m) + u_0^2)$$

Where the pre-factor 2^{2^m} is used to make all coefficient integral (I_m contains rational non-integral coefficients).
We still need to find the bounding polynomial $E(a, x)$. For that polynomial we can just try and find the maximum of $x(1 + M^2(a, u_1, ..., u_n))$, because in expression (44) the $u_1, ..., u_n$ are bounded by that maximum. We can for instance just take $E(a, x) = x(1 + N(a, x))$ with N equal to be the square of M with all signs turned positive and for all variables $y, u_1, ..., u_n$ we substitute an x. This makes E at least as large as the maximum discussed before, and so it also bounds $u_1, ..., u_n$ (meaning there are no solutions for u_i larger than E).
This concludes the proof of the Single-fold Davis Theorem.

□

Now for something different, remember that the Chinese remainders theorem can be stated in such a way that it is single-fold:

Single-fold Chinese remainders theorem: *For all pairwise relatively prime positive numbers $d_1, ..., d_t$ and integers $a_1, ..., a_t$ there is only one a such that $0 \geq a < d_1, ..., d_t$ and $a \equiv a_i \ mod \ d_i$ for all $1 \leq i \leq t$.*

10.2 The proof

We will now prove the single-fold DPR-theorem. Take a recursively enumerable predicate $P(a)$ and take D and E to be as in the single-fold Martin Davis theorem. Define $F(a, x)$ as the polynomial created from $D(a, x, y, u_1, ..., u_m)$ with all minus signs turned into plus signs and all variables except a and x replaced with $x + E(a, x)$.
We will also define polynomials D_i by expanding D at $y = -1$, such that $D(a, x, y, u_0, ..., u_m) = \sum_{i=0}^{s} D_i(a, x, u_0, ..., u_m)(y+1)^i$, where we take s to be the degree of y in D. We define a new polynomial $R(a, x, r, u_0, ..., u_m) = \sum_{i=0}^{s} D_i(a, x, u_0, ..., u_m)(-r)^{s-i}$.

We are going to prove that the following system of four exponential diophantine relations give us a single-fold representation of our recursive enumerable set $P(a)$. The unknowns are $x, r, q, s_1, s_2, ..., s_m$:

(I) $r = (E(a,x) + F(a,x) + x + 1)!$
(II) $q = \prod_{i=0}^{x}(1 + r(i+1))$
(III) $(\forall\ 0 \leq t \leq m) : [[q \mid \prod_{i=0}^{E(a,x)}(s_t - i)] \quad \& \quad [s_t < q]]$
(IV) $R(a, x, r, s_0, ..., s_m) \equiv 0 \bmod q$

Notice that both (II) and (III) use products with variable indexes (x in (II) and $E(a,x)$), we have shown in Lemma 4.4 that these are exponential diophantine. Also notice that though (III) contains a universal quantifier, it is bounded by a constant so it is actually just a system of m exponential diophantine equations. So with previous results we know that this system is exponential diophantine. Now let us prove it is a single-fold representation of $P(a)$.

Proof:
• First, let us prove that the system implies $P(a)$. Take a natural number a and assume there are $x, r, q, s_0, ..., s_m$ such that the four relations are valid. Let y be a natural number smaller or equal than x. Let p be a prime divisor of $1 + r(y+1)$. According to (II) and (III), $p | \prod_{i=0}^{E(a,x)}(s_t - i)$ for all $0 \leq t \leq m$.
So there are $u_0, ..., u_m$ for which $p|(s_t - u_t)$ and $u_t \leq E(a,x)$ for all $0 \leq t \leq m$. Combining this result with (II) and (IV) we get: $R(a, x, r, u_0, ..., u_m) \equiv 0 \bmod p$.
So $0 \equiv R(a, x, r, u_0, ..., u_m) \equiv \sum_{i=0}^{s} D_i(a, x, u_0, ..., u_m)(-r)^{s-i} \equiv \sum_{i=0}^{s} D_i(a, x, u_0, ..., u_m)(-r)^{s-i}(y + 1)^s \equiv \sum_{i=0}^{s} D_i(a, x, u_0, ..., u_m)(y+1)^i \equiv D(a, x, y, u_0, ..., u_m) \bmod p$.
From (I) we know that $p > F(a,x) \geq |D(a, x, y, u_0, ..., u_m)|$. So indeed $D(a, x, y, u_0, ..., u_m) = 0$ and thus $P(a)$ is valid (because $D = 0$ was its representation).

• Now for the converse, assume a as an element of the recursively enumerable with predicate P (so $P(a)$ is true). By our equivalent statements in the refined Davis theorem, we know that there are x and there are $u_{(0,y)}, ..., u_{(m,y)}$ such that for all $0 \leq y \leq x : u_{(t,y)} \leq E(a,x)$ for all $0 \leq t \leq m$ and $D(a, x, y, u_{(0,y)}, ..., u_{(m,y)}) = 0$.
Now we choose r and q such that (I) and (II) are valid. Just like in our original proof (the not single-fold proof), we know that for $0 < y_1 < y_2 \leq m$, $1 + r(y_1 + 1)$ and $1 + r(y_2 + 1)$ are relative prime (you can simply prove this).
So with the Refined Chinese remainder theorem we can find $s_0, ..., s_m$ such that $s_t \leq q$ and $s_t \equiv u_{(t,y)} \bmod (1 + r(y+1))$ for all $0 \leq t \leq m$ and $0 \leq y \leq x$. With this (III) is correct.
With our previous results, we see that for all y not exceeding m:
$0 \equiv D(a, x, y, s_0, ..., s_m) \equiv \sum_{i=0}^{s} D_i(a, x, u_0, ..., u_m)(y+1)^i \equiv \sum_{i=0}^{s} D_i(a, x, u_0, ..., u_m)(y+1)^i(-r)^s \equiv \sum_{i=0}^{s} D_i(a, x, u_0, ..., u_m)(-r)^{s-i} \equiv R(a, x, r, s_0, ..., s_m) \bmod (1 + r(y+1))$. And because $(1 + r(y+1))$ is relative prime for different y, we can conclude that (IV) is also correct. So there is a solution for the system of four equations.

• We can conclude that the system represents $P(a)$, but is it single-fold? Let a satisfy $P(a)$ and take $x, r, q, s_0, ..., s_m$ and $X, R, S_0, ..., S_m$ to be two sets of variables satisfying the relations I-IV.
We know that $(\forall y \leq x)(\exists u_0, ..., u_m)[D(a, x, y, u_0, ..., y_m) = 0]$ and $(\forall y \leq X)(\exists u_0, ..., u_m) : [D(a, X, y, u_0, ..., u_m) = 0]$.
According to the refined Davis theorem we have that $(\exists! k)(\forall y \leq k)(\exists u_0, ..., u_m) : [D(a, x, y, u_0, ..., u_m)]$ and so we can derive that $x = X$. So now we can find from (I) and (II) that $r = R$ and $q = Q$.
Let us now assume that there is a j such that $s_j \neq S_j$. By assumption, $s_j < q$ and $S_j < q$, so there is

a prime p and a positive number d such that $p^d|q$ and $s_j \not\equiv S_j \bmod p^d$, and so $p^d|\prod_{i=0}^{E(a,x)}(s_j - i)$ and $p^d|\prod_{i=0}^{E(a,x)}(S_j - i)$.
From (I) and (II) we find that $p > E(a,x)$ which means that there are u_j and U_j such that $p^d|(s_j - u_j)$, $p^d|(S_j - U_j)$, $u_j \leq E(a,x)$ and $U_j \leq E(a,x)$. Because $s_j \not\equiv S_j \bmod p^d$ we find that $u_j \neq U_j$. Take the other u_i and U_i with $i\epsilon\{0,...,j-1,j+1,...,m\}$ such that $p|(s_t - u_t)$ and $u_t \leq E(a,x)$ for all $0 \leq t \leq m$. As before, in our proof that (I-IV) implies P(a), we can derive that $D(a,x,y,u_0,...,u_m) = 0 = D(a,x,y,U_0,...,U_m)$. But according to the refined Martin Davis theorem, we know that $(\forall y \leq x)(\exists! u_1,...,u_m) : [D(a,x,y,u_1,...,u_m) = 0]$, so $u_i = U_i$ for all $i\epsilon 0,1,...,m$. But that is in contradiction with $u_j \neq U_j$. So we can conclude that there is no j such that $u_j \neq U_j$.
Conclusion, for all a satisfying $P(a)$ there is but one solution of (I-IV) in the unknowns $r, x, s_0, ..., s_m$.

□

And so we have found a single-fold exponential diophantine representation of an arbitrary recursively enumerable set. And because of bijections between different dimensional sets, we can also represent any recursively enumerable relation the same way.

11 Implications of finite-fold exponentiation

Now that we know that all r.e. are single-fold exponential diophantine, a single-fold or finite-fold diophantine representation of exponentiation would give us respectively a single-fold or finite-fold diophantine representation for an arbitrary r.e. set. However, as of yet this representation has not been found. The salvaged Martin Davis theorem in chapter 7 however gives us a bit of hope for the possibility of finite exponentiation.

But what does it actually mean when a diophantine equation has a finite number of solutions? Let us take $D(a_1,...,a_n) = 0$ with D a integral polynomial. If we know that it only has a finite number of solutions, we know that the number of solutions is smaller than a certain number c. We can also find a bound for the variables, a constant b such that all solutions of $D = 0$ satisfy $a_1 < b$,...,$a_n < b$. Or in other words, $\forall a_1, a_2, ..., a_n$, if for some i, $a_i \geq b$ then $D(a_1, a_2, ..., a_n) \neq 0$.
If we know the bound b, it is possible to check how many solutions of $D = 0$ there are by just trying all possible combinations of $a_1, ..., a_n$ smaller than b.
But if we know the bound for the number of solutions of $D = 0$ (or even if you exactly know the number of solutions) then there is no general method to find a bound b for the unknowns.
So having a bound for the variables, you can find all solutions of the equation, that is why such information is called an *effective estimate* of the solutions of the equation. A bound for the number of solutions is called a *non-effective estimate*, because with it you may still be unable to find all the solutions. Therefore it is better to have an effective estimate than to have a non-effective one.

A classic example from the past is a theorem from Axel Thue in 1909, which states that if we have a irreducible binary form F with a degree of at least 3, then for all integers a we have that $F(x,y) = a$ only has a finite number of solutions in the unknowns x and y. This is a typical non-effective estimate. Only in 1968 an effective estimate was found by Alan Baker.
It is still not known if all equations with a non-effective estimate also have an effective estimate. Till this day, no example of an equation with non-effective estimate without the possibility of an effective estimate has been found.
The next two results were originally discussed in [17].

Non-effectiveness

Say that we have proven that all recursive enumerable sets are finite-fold diophantine. This would mean that we have a non-effective estimate of the diophantine equation which represents that set. But if we take a recursive enumerable, but not recursive set S, and look at its representation $D(x, a_1, ..., a_n)$ we see something interesting. Because S is not recursive, we can find an element $x \epsilon \mathbb{N}$ of which we know that there is no recursive way of determining if $x \epsilon S$. Now, let us assume $D(x, a_1, ..., a_n) = 0$ has an effective estimate for its solutions in $a_1, ..., a_n$. Then with that estimate, we can try all possible combinations of these variables within the bound and check within a finite amount of time whether $x \epsilon S$. But that is in contradiction with the assumption that there is no recursive way of determining that. We can conclude that the diophantine equation $0 = P(a_1, ..., a_n) := D(x, a_1, ..., a_n)$ has no effective estimate. This gives us an example of what we discussed before:

Conjecture corollary: *If exponentiation is finite-fold diophantine, then there are diophantine equations with a non-effective estimate but without the possibility of ever finding an effective estimate.*

Effectiveness
Now let us assume that it is not possible to create a finite-fold diophantine representation of exponentiation, so we have found a recursive enumerable set which does not have a finite-fold diophantine representation. This would mean that all possible ways to construct such a representation are impossible. Recall the Julia Robinson prerequisites:

Julia Robinson prerequisites theorem: $\{< a, b, c > | a = b^c\}$ *is finite-fold diophantine if there is a Diophantine equation* $J(u, v, x_1, ..., x_n) = 0$ *(having for every* u *and* v *only a finite number of solutions) with the following two properties:*
-$\forall k$ *there is a solution with* $v > u^k$
-In every solution $v < u^u$

Julia Robinson was able to improve this result using super powers. Take $u * m$ to be the m-th super power of u. With this definition she proved the following:

Improved Julia Robinson prerequisites theorem: $\{< a, b, c > | a = b^c\}$ *is finite-fold diophantine if there is a Diophantine equation* $J(u, v, x_1, ..., x_n) = 0$ *(having for every* u *and* v *only a finite number of solutions) with the following two properties:*
-$\forall k$ *there is a solution with* $v > u^k$
-There is a natural number m *such that in every solution,* $v < u * m$

If we have a counter-example, then it is impossible to find a finite-fold diophantine representation of exponentiation, and so it would also be impossible to construct any equation with the properties in the theorems of Julia Robinson. So we get the result:

Conjecture corollary II: *If there is a recursive enumerable set which does not have a finite-fold diophantine representation, then for all Diophantine equations* $J(u, v, x_1, ..., x_n) = 0$ *having for every* u *and* v *only a finite number of solutions and for which there is a* m *such that* $v < u * m$ *for all solutions, then there is a* k *such that* $v < u^k$.

12 Martin Davis-like equations

We know a lot about diophantine equation with at most 2 unknowns and at most a degree of 3. Beyond those values, things get perilous. Those equations become way too unpredictable. A particular equation

that has peeked the interest of mathematicians in the last couple of decades is the equation that Martin Davis used in his attempt to prove that exponentiation is diophantine. He assumed that the equation $9(u^2+7v^2)^2-7(r^2+7s^2)^2=2$ only has the trivial solution $u=1,v=0,r=1,s=0$. But Oskar Herrmann found its first non-trivial solution in 1971 ([9]), and in 1995 Daniel Shanks and Samuel Wagstaff found 48 more solutions ([15]).
As discussed before, we can salvage Martin Davis' proof to get the result: Exponentiation is single-fold diophantine if $9(u^2+7v^2)^2-7(r^2+7s^2)^2=2$ only has a finite number of solutions. Still, a lot of arguments have been given saying that the equation has an infinite number of solutions, though it has never been proven. The solution space of this equation seems to be teetering on the edge of finiteness and infiniteness.
In this chapter we will look at a more general equation: $a(u^2+Nv^2)^2-b(r^2+Ns^2)^2=a-b$, with parameters a,b,N ($gcd(a,b)=1$, N does not contain any squares) and unknowns u,v,r,s. We will call this type of equation a Martin Davis-like equation. For all choices of parameters, we have the trivial solution $(1,0,1,0)$.

12.1 Combination of two equations

A Martin Davis-like equation is a composition of two parts.
One part is the Pell-like equation: $ax^2-by^2=a-b$, with parameters a and b, and unknowns x and y. Though the solutions of these Pell-like equations can not be described generally (unlike the Pell equations), there are well known methods of finding generating a lot of solutions. One need just multiply both sides with a to find $(ax)^2-aby^2=a(a-b)$. With $z=ax$ we get the Pell-like equation $z^2-aby^2=a(a-b)$. The solutions can be described as the elements of $\mathbb{Z}[\sqrt{ab}]$ with norm $a(a-b)$. So if we have an element of that extension with norm 1 and one with norm $a(a-b)$, then we know that their multiplication is also a solution. So a good way of finding a lot of solution is to first find the general sequence of solutions of the equation $z^2-aby^2=1$ (these are discussed to a great extend in the chapter about Pell equations). Then one searches for solutions of our original equation, each of those generating an infinite sequence of solutions which may or may not be independent. So if $(z,y)=(u,v)$ is the first non-trivial solution of $z^2-aby^2=1$ and $(z,y)=(r,s)$ is a solution of $z^2-aby^2=a(a-b)$, then for all $n>1$ we have that there is a solution (z,y) of $z^2-aby^2=a(a-b)$ with $x+\sqrt{ab}=(u+\sqrt{ab})^n(r^2+\sqrt{ab}s^2)$ (for each n there is a different solution). Notice that $a|a(a-b)$ and $a|aby^2$, so $a|z^2$ in all solutions of the equation. So to find a solution of $ax^2-by^2=a-b$, we just need to take $(x,y)=(z/a,y)$ for any solution (z,y) of $z^2-aby^2=a(a-b)$ previously discussed.

The second part is the representation by u^2+Nv^2. This was partly discussed in the chapter of Martin Davis' proof for $N=7$. For that case, it was proven that for any natural number x, if for all prime dividers p of x we have that: $\left(\frac{p}{N}\right)=-1$ implies that p divides x an even amount of times, then x can be represented by u^2+Nv^2. This statement is also true for $N=2$ and $N=3$, this can be proven the same way.
The Martin Davis-like equation is now a question of which solutions of the equation $ax^2-by^2=a-b$ have coördinates which can both be represented by u^2+Nv^2.

12.2 Early Solutions

I will now show you a table containing some solutions of the Martin Davis-like equation. Each box contains all non-trivial solutions of the equation with $u,v,r,s\leq 2500$ and with certain choice of parameters a, b and N. On the left hand side the values of a,b are displayed, they contain all $0<b<a\leq 12$ with $gcd(a,b)=1$. On top the value of N is given, with all natural numbers below 12 not containing a square, so $N=1,2,3,5,6,7,10,11$. For $N=1$, only the solutions with $u\geq v$ and $r\geq s$ are displayed to avoid any unnecessary use of space (if one wants all solutions for $N=1$, just

consider the fact that you can swap both u and v, and you can swap r and s).

The solutions seem to behave very irregularly. For some parameters the solutions appear on a regular interval, for some other parameters the equation does not have any solutions below 2500 and for some parameters the equation has a lot of solutions but only in a small interval. This behavior does not seem to have any correlation with the choice of parameters. We see that for $a = 9$ and $b = 7$ we have no solutions for any choice of N, not just for $N = 7$ (where the first non-trivial solutions has an u of 525692038369576), so the Pell-like equation $9x^2 - 7y^2 = 2$ does not seem to be as susceptible to representations as other Pell-like equations in the table. Though for other a and b it can be seen that most solutions are just different representations of the same solution of the Pell-like equation $ax^2 - by^2 = a - b$. So, it seems that most representable solutions have more than one representation. Still, it will be difficult to state something concrete about the finiteness of these equations, any solution of the Pell-like equation can only be represented a finite number of times, so the question is whether there are an infinite amount of representable solutions. This question is yet to be solved for $a = 9$, $b = 7$ and $N = 7$, and it might be equally as difficult for other choices of parameters.

a	b	N = 1	N = 2	N = 3	N = 5	N = 6	N = 7	N = 10	N = 11
2	1	2 5 4 5			3 2 6 1	11 12 23 12 11 12 37 2 31 2 23 12 31 2 37 2	13 0 8 5 181 10 83 76 181 10 211 20 197 970 988 1095 2101 562 988 1095		
3	1	3 12 3 16 3 12 11 12	3 1 1 3 41 15 53 21 1213 1464 341 2220 1213 1464 1097 2094 2131 780 341 2220 2131 780 1097 2094 2207 666 341 2220 2207 666 1097 2094 2369 270 341 2220 2369 270 1097 2094	16 25 4 35	6 77 73 96 6 77 127 84 81 68 73 96 81 68 127 84		2 9 17 10 2 9 31 2	1 1 3 1 21 13 9 19 111 758 539 984 531 740 539 984 911 702 539 984 1469 600 539 984	
3	2	5 8 3 10 440 813 10 1023 440 813 225 998	1 2 3 1 3 0 3 1 3 66 59 60 3 66 103 6 23 64 59 60 23 64 103 6 39 60 59 60 39 60 103 6 61 50 59 60 61 50 103 6 67 46 59 60 67 46 103 6 87 24 59 60 87 24 103 6 89 20 59 60 89 20 103 6 93 6 59 60 93 6 103 6	787 280 373 550 787 280 971 186	3 4 8 3		3 0 2 1	3 0 1 1 73 90 61 101 73 90 229 73 213 64 61 101 213 64 229 73	3 0 0 1
4	1								
4	3	12 187 12 201 12 187 84 183 12 187 96 177 12 187 111 168 72 173 12 201 72 173 84 183 72 173 96 177 72 173 111 168 83 168 12 201 83 168 84 183 83 168 96 177 83 168 111 168 132 133 12 201 132 133 84 183 132 133 96 177 132 133 111 168							
5	1	1 1 0 2 2 3 2 5 8 13 11 20 34 55 18 95 41 50 18 95 610 987 1018 1405 762 875 1018 1405	0 1 2 0 4 3 2 6 15 2 3 16	25 18 52 17		71 108 119 160 71 108 181 150 71 108 245 134 71 108 295 116 169 88 119 160 169 88 181 150 169 88 245 134 169 88 295 116 245 50 119 160 245 50 181 150 245 50 245 134 245 50 295 116	15 14 22 21 53 14 93 10 59 10 93 10		
5	2			2 3 1 4 2 3 7 0 1169 332 181 940 1225 256 181 940		5 1 5 2 5 1 7 0 853 402 1175 466 1177 228 1175 466	0 1 2 1	15 2 13 5	
5	3			1 12 14 11 1 12 22 5 2 1 3 0 41 24 63 12 47 20 63 12	23 24 14 29 23 24 39 24 23 24 49 20 23 24 66 3 58 3 14 29 58 3 39 24 58 3 49 20 58 3 66 3	1 1 3 0 367 113 479 85 367 113 521 15 433 63 479 85 433 63 521 15	0 1 3 0		
5	4		3 2 1 3						417 380 980 303 417 380 1000 297
6	1	19 80 81 100	81 10 19 90	0 1 2 1 160 29 22 151 160 29 158 121 160 29 230 73 160 29 262 9 671 266 1147 320 671 266 1189 264 769 154 1147 320 769 154 1189 264	7 2 13 0 8 1 13 0 69 20 71 48		1 2 8 1 26 1 35 8	1 26 99 26	5 2 13 0
6	5	10 19 8 21 10 19 12 19			21 2 10 9			219 132 7 156 219 132 263 132 219 132 403 90 219 132 493 6 471 6 7 156 471 6 263 132 471 6 403 90 471 6 493 6	
7	1	1 2 2 3	3 25 17 39 193 60 49 240 193 60 293 126	10 5 10 11		5 5 13 7 11 3 13 7 13 1 13 7 175 48 1 140 175 48 305 64	0 5 20 3 2 1 1 2	7 11 21 17 203 18 31 108 203 18 171 94	
7	2	8 25 8 35 17 20 8 35		2 1 1 2			4 1 6 1 72 47 190 19 100 39 190 19	7 8 17 10 23 4 17 10 459 202 39 340 459 202 169 336 459 202 781 234 459 202 909 182 689 120 39 340 689 120 169 336 689 120 781 234 689 120 909 182	
7	3	3 100 40 117 6 20 15 21	2 0 2 1 53 60 121 18 143 735 1097 489	4 5 8 5 8 3 8 5 91 24 67 60 436 551 1288 87	2 0 1 1 98 9 122 9	2 0 0 1 97 10 17 50		1 3 7 3 9 1 7 3 57 26 123 4 747 233 701 345	
7	4	129 200 20 273 135 196 20 273		223 48 127 140 233 28 127 140		13 3 1 7 13 3 17 1		159 56 263 24 209 36 263 24	

a	b	N = 1	N = 2	N = 3	N = 5	N = 6	N = 7	N = 10	N = 11
7	5							31 42 87 38 31 42 137 18 51 40 87 38 51 40 137 18 129 14 87 38 129 14 137 18 131 12 87 38 131 12 137 18	
7	6		5 0 3 3 5 0 5 1 365 390 9 486 365 390 139 476 365 390 315 432 365 390 425 382 365 390 439 374 365 390 471 354 365 390 629 136 365 390 645 168 365 390 651 156 365 390 681 66	5 0 0 3 65 380 45 396 65 380 531 252		25 52 7 55 43 50 7 55 55 48 7 55 107 30 7 55			5 0 4 1
8	1	0 8 9 10 1 1 1 2 448 837 391 1548 448 837 616 1473	2 0 3 1 6 7 19 3 9 115 273 16 159 25 273 16	4 4 13 2 8 0 13 2	8 0 1 6	607 298 689 588 607 298 1549 158	2 0 2 1 9 10 47 0 22 61 71 100 23 6 47 0 134 35 71 100	2 0 1 1 268 91 159 203 268 91 239 195	2 0 0 1
8	3	2 2 2 3 46 75 79 80	0 1 1 1	2 5 9 4 4 1 2 3	64 27 111 8				
8	5	0 2 1 2 814 1095 648 1391 814 1095 724 1353 1830 2218 2111 2450	4 3 5 3		2 0 0 1		12 1 4 5	208 24 249 1	20 9 7 12
8	7								
9	1								
9	2	0 5 2 7 3 4 2 7	1 2 1 3 3 0 1 3 7 20 1 30 29 2 1 30	3 0 4 1 9 16 37 12	2 13 26 15 23 8 26 15		5 0 5 2 13 64 97 86 13 64 209 50 83 56 97 86 83 56 209 50	3 0 3 1	5 0 3 2
9	4								
9	5	5 16 4 19 5 16 11 16 180 241 17 348 180 241 172 303	2 1 0 2 2 31 28 30 2 31 44 18 26 25 28 30 26 25 44 18 42 9 28 30 42 9 44 18 173 174 19 246 173 174 109 234				1763 404 1728 623 1763 404 2388 7 2059 40 1728 623 2059 40 2388 7		
9	7								
9	8					417 432 263 466 417 432 551 422 417 432 569 418 417 432 611 408 417 432 857 326 417 432 1117 144 417 432 1123 136 417 432 1171 12 543 408 263 466 543 408 551 422 543 408 569 418 543 408 611 408 543 408 857 326 543 408 1117 144 543 408 1123 136 543 408 1171 12 753 348 263 466 753 348 551 422 753 348 569 418 753 348 611 408 753 348 857 326 753 348 1117 144 753 348 1123 136 753 348 1171 12 1137 12 263 466 1137 12 551 422 1137 12 569 418 1137 12 611 408 1137 12 857 326 1137 12 1117 144 1137 12 1123 136 1137 12 1171 12	97 64 104 65 127 56 104 65		
10	1	2 3 4 5 7 30 20 51 15 136 95 224 15 136 140 199 18 25 20 51 80 111 95 224 80 111 140 199 459 1076 1404 1535 684 949 1404 1535	1 1 1 2 1 1 3 0 275 804 1507 1014 787 612 1507 1014	0 1 3 0 5 0 2 5 6 5 18 3 19 14 53 8 29 6 53 8 372 85 642 177		1 2 5 3 5 0 5 3	5 0 4 3		
10	3	1 2 0 3 3 424 121 560 3 424 220 529 32 37 12 65 32 37 20 63 96 413 121 560 96 413 220 529 171 388 121 560 171 388 220 529 252 341 121 560 252 341 220 529 461 970 235 1432 461 970 557 1340	9 34 29 42 9 34 61 18	1 6 14 1	0 1 2 1 0 1 3 0	101 84 165 107 229 4 165 107			
10	7	4 5 0 7 245 414 45 524 245 414 160 501 250 411 45 524 250 411 160 501	3 4 7 0		6 1 2 3 6 1 7 0			1 2 3 2 1 2 7 0	
10	9	6 37 16 35 26 27 16 35 228 1405 249 1440 228 1405 324 1425 240 1403 249 1440 240 1403 324 1425 460 1347 249 1440 460 1347 324 1425 872 1125 249 1440 872 1125 324 1425		5 2 6 1 85 124 214 59	35 6 6 17	83 88 235 13			

a	b	N = 1	N = 2	N = 3	N = 5	N = 6	N = 7	N = 10	N = 11
11	1			1 2 4 3 4 9 28 5 16 1 28 5 62 21 95 52		11 29 101 34 41 130 395 176 41 130 559 70 265 74 395 176 265 74 559 70	0 1 4 1 8 27 127 12 77 84 424 23	3 5 7 9 13 3 7 9	
11	2	7 8 3 16 7 8 11 12	9 10 9 17	3 0 3 2	2 1 1 2 2 1 4 1 3 0 1 2 3 0 4 1	9 24 9 37 9 24 57 29 9 24 81 17 9 24 87 11	13 4 22 5	11 4 13 7 31 66 49 101 31 66 119 95 211 0 49 101 211 0 119 95	
11	3	33 1844 1048 2327 548 1761 1048 2327 1080 1495 1048 2327	1565 690 249 1796 1565 690 1671 1364	29 16 3 32 29 16 27 28		11 8 31 1 17 6 31 1 505 368 717 505 505 368 1245 287			1745 180 1143 688
11	4	15 356 146 435 15 356 270 371				5 7 23 0 13 5 23 0	12 5 9 8 12 5 23 0 16 3 9 8 16 3 23 0		
11	5	7 10 5 14 7 10 10 11	23 114 67 132 23 114 175 66 139 60 67 132 139 60 175 66				1 2 6 1		
11	6	7 8 3 12 17 120 17 140 55 108 17 140	9 4 5 8 9 4 9 6 9 4 11 4 387 938 1485 436 777 808 1485 436 1095 596 1485 436 1347 218 1485 436	47 0 54 5				107 18 23 44 117 10 23 44	
11	7	2 2 1 3 460 481 16 745 460 481 380 641					8 9 28 1 71 80 44 93 71 80 152 75 97 76 44 93 97 76 152 75 167 56 44 93 167 56 152 75 223 4 44 93 223 4 152 75	589 98 211 226 589 98 659 110	
11	8	2 5 3 5 20 105 74 89 47 96 74 89 72 79 74 89		169 196 382 87 353 80 382 87		305 92 409 15 365 42 409 15			639 610 2278 90
11	9		19 3 9 13	4 1 3 2 67 32 34 49 67 32 74 31				17 3 13 5	
11	10	11 40 19 38	3 4 5 3		21 16 0 19				
12	1	0 31 25 52 1 2 1 4 2 11 12 17 5 10 12 17	31 0 21 38	3 0 2 3 17 22 22 43 17 22 62 27	31 0 57 4	3 0 5 1	31 0 23 20	31 0 37 14	
12	5		3 1 3 2						
12	7	2 3 1 4		7 4 10 3	43 42 62 45 43 42 118 3 92 21 62 45 92 21 118 3	1 4 11 1	27 10 32 11		
12	11	25 38 15 44			33 14 46 3				1 2 6 1 683 596 1103 552 683 596 2137 12 1011 552 1103 552 1011 552 2137 12 2067 96 1103 552 2067 96 2137 12 2069 92 1103 552 2069 92 2137 12 2091 12 1103 552 2091 12 2137 12

13 Examples of specific diophantine representations

Let us end this paper with something a bit less abstract.
When the DPRM-theorem was proven, many mathematicians sought specific examples of diophantine representations. These could be used to represent mathematical statements, even open conjectures. This chapter will discuss some of those.

In the year 1976, James P. Jones found the diophantine representation of the set of prime numbers ([12]). He proved that they were represented by the equation with unknowns $a, b, c, ..., z$ (alphabet without k) and parameter k:

$$[wz+h+j-q]^2+[(gk+2g+k+1)(h+j)+h-z]^2+[2n+p+q+z-e]^2+[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2+[e^3(e+2)(a+1)^2+1-o^2]^2+[(a^2-1)y^2+1-x^2]^2+[16r^2y^4(a^2-1)+1-u^2]^2+[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2+[n+l+v-y]^2+[(a-1)l^2+1-m^2]^2+[ai+k+1-l-i]^2+[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2+[q+y(a-p-1)+a(2ap+2a-p^2-2p-2)-x]^2+[z+pl(a-p)+t(2ap-p^2-1)-pm]^2=0$$

This system has a solution in his unknowns for a certain value of k if and only if $k+2$ is a

prime. For simplification we will write this equation as $P(k, a, b, c, ..., z) = 0$.
With this equation we can rewrite a lot of problems in number theory that are not even about diophantine equations in such a way that they do coincide with the solvability of some diophantine equation.

Goldbach conjecture *Every even number greater than 2 can be written as the sum of two primes.*
This question is equivalent to the following statement: For all non-negative n, the following diophantine equation with unknowns $p_1, p_2, a_1, a_2, ..., a_{25}, b_1, b_2, ..., b_{25}$ has a solution:

$$[2n - (p_1) - (p_2)]^2 + [P(p_1 - 2, a_1, a_2, ..., a_{25})]^2 + [P(p_2 - 2, b_1, b_2, ..., b_{25})]^2 = 0$$

has a solution.

Legendre's conjecture *There is a prime number between every two consecutive squares*
This is equivalent with the statement: For all non-negative n, the following diophantine equation with unknowns $p, d, e, a_1, a_2, ..., a_{25}$ has a solution:

$$[n^2 + d - p]^2 + [(n + 1)^2 - e - p]^2 + [P(p - 2, a_1, a_2, ..., a_{25})]^2 = 0$$

Twin primes conjecture *There are infinitely many twin primes.* Note that the question of there being infinitely many of something in an ordered system with a minimum is equivalent to the question of there always being one higher than the ones you already got.
With that in mind we see that the conjecture is equivalent to the following statement: For all non-negative n, the following diophantine equation with unknowns $p, d, a_1, a_2, ..., a_{25}, b_1, b_2, ..., b_{25}$ has a solution:

$$[n + d - p]^2 + [P(p - 2, a_1, a_2, ..., a_{25})]^2 + [P(p, b_1, b_2, ..., b_{25})]^2 = 0$$

There are many conjectures talking about the existence of infinitely many primes with a certain extra property. As long as this property is diophantine, one can obviously represent the conjecture in a diophantine way. Say the property can be represented by a integral polynomial $D(x, a_1, ..., a_n)$ having a zero in $a_1, ..., a_n$ if and only if x has the property.

There are infinitely many primes with a property represented by $D = 0$ if and only if for every non-negative n the following diophantine equation with unknowns $p, a, a_1, a_2, ..., a_{25}, b_1, b_2, ..., b_k$ has a solution

$$[n + 2 + a - p]^2 + [D(p, b_1, ..., b_k)^2 + [P(p - 2, a_1, a_2, ..., a_{25})]^2 = 0$$

Besides the prime number representation, James P. Jones also found other representations ([11]). One of the more simple diophantine representation is the one for the fibonacci numbers: A number y is in the fibonacci sequence if and only if there is an x such that $(y^2 - xy - x^2)^2 - 1 = 0$. This gives us a representation of the following conjecture:

Fibonacci prime conjecture: *There are infinitely many primes in the Fibonacci sequence*

One should also not forget the central result of this paper, the fact that exponentiation is diophantine. With that representation we can easily represent the following conjecture.

Mersenne prime conjecture: *There are infinitely many primes of the form* $2^n - 1$

14 Discussion and conclusion

14.1 Discussion

To prove that all recursively enumerable sets are single-fold or finite-fold diophantine, we have to prove that the exponential relation is respectively single-fold or finite-fold diophantine. But how would we go about doing that?
One possible way to go is to prove that $9(u^2 + 7v^2)^2 - 7(r^2 + 7s^2)^2 = 2$ only has a finite number of solutions. To this extend, it might be useful to study the Martin Davis-like equation in order to discover some deeper properties we have not yet found. Of course, the assumption is a much stronger statement than the thing we want to prove, so there is a chance that it is not true while exponentiation is still single-fold diophantine. This might discourage people to study it. Still, the Martin Davis-like equation are very interesting in their own right, they may be a gateway to new theories so I would encourage people to look into them.
The second way to go is to change Matiyasevich's proof in such a way that it also contains a single/finite-fold nature. This might happen by finding the correct bound for its unknowns. Matiyasevich's proof has also been used to create alternative proofs having roughly the same steps. Those could also be used as a starting point. The problem is however, that many people have already attempted to improve these, including Matiyasevich himself. From this fact we can conclude that it will be very difficult to go this route.
A more general way would be to try and prove the existence of a polynomial $J(u, v, x_1, ..., x_n)$ which satisfies the Julia Robinson prerequisites and which also is finite or single-fold with u and v as parameters and $x_1, ..., x_n$ as unknowns. This would require a lot of ingenuity, seeing that most infinite-fold proofs use many steps that only make sense when the whole argument is made. A lot of leaps must be made demanding a lot of trial and error in using many different equations.
A proof might even fall from the sky, as someone might find out about the exponential nature of some single-fold diophantine equation he or she was studying. It is difficult to say.

14.2 Conclusion

We have seen that all recursively enumerable relations are diophantine and that they are single-fold exponentially diophantine. We have also seen how far we are in proving that they are single-fold diophantine and the consequences that it may bring. But the last few years, there has not been much improvement in the search of the single-fold representation of the exponential relation. Both Matiyasevich's and Martin Davis' proof use very specific constructions of various diophantine equations, if one wants to change a small thing you will have to change the whole proof.
I was not able to change Martin Davis proof in such a way that a different assumption arose than: $9(u^2 + 7v^2)^2 - 7(r^2 + 7s^2)^2 = 2$ has only a finite number of solutions. So Davis' constructive and thereby single-fold method of proving that exponentiation is diophantine seems to be forever tied to that equation. But an analysis of the equation by many different mathematicians show that the validity of the assumption is doubtful. Further study of this equation must be done to check the validity of the assumption.
On the other hand, the proof of Matiyasevich uses modular equations to such an excessive extend that even after many years of work from various different mathematicians, we still do not have a bound to the unknowns used in Matiyasevich's diophantine representation of exponentiation.
In my study, I discovered that all publications regarding this conjecture uses the Pell equation in one way or another. There may be different diophantine equations that can also be used, though that might be even more difficult seeing that the Pell equations are very simple in construction.
Let us not forget that it took many years before somebody was able to prove that exponentiation is diophantine and many more years have passed since. It might take a long time before the conjecture

is proven or disproven. A proof might be just around the corner, or maybe there is no proof at all. Whatever the result is, it will either take a mathematical genius or a lot of luck to assign a truth value to the statement: All recursive enumerable sets are single-fold diophantine.

References

[1] David Hilbert, *Mathematische Probleme. Vortrag, gehalten auf dem internationalen Mathematiker-Kongress zu Paris 1900*, Nachtrichten von der K. Gesellschaft der Wissenschaften zu Gotingen, 1900, pp. 253-297

[2] Kurt Gödel, *Über formal unentscheidbare Satze der Principia Mathematica und verwandter Systeme I*, Monatshefte für Mathematik und Physik, vol. 38 (1931), pp. 173-198.

[3] J. B. Rosser, *Extensions of some theorems of Gödel and Church*, Journal of symbolic logic, vol. 1 (1936), pp. 87-91

[4] Julia Robinson, *Existential definability in Arithmetic*, 1951

[5] Martin Davis, *Arithmetical Problems and Recursively Enumerable Predicates*, Journal of Symbolic Logic, Vol 18, No. 1 (Mar. 1953), pp 33-41

[6] Martin Davis, Hilary Putnam and Julia Robinson, *The Decision Problem for Exponential Diophantine Equations*, Annals of Mathematics, Second Series, Vol. 74, No. 3 (Nov. 1961), pp. 425-436

[7] Martin Davis, *One equation to rule them all*, 1968

[8] Yuri V Matiyasevich, *Enumerable sets are Diophantine*, Soviet Math Dokl. 11 (1970), pp. 354-358

[9] Oskar Herrmann, *A non-trivial solution of the diophantine equation* $9(x^2+7y^2)^2-7(u^2+7v^2)^2=2$, Computers in Number theory, Academic Press, London, 1971, page 207-212

[10] Yuri V Matiyasevich, *Existence of Non-effectivizable estimate in the theory of exponential diophantine equations*, LOMI, Volume 40, 1974, pp. 7793

[11] James P. Jones, *Diophantine representation of Fibonacci numbers*

[12] James P. Jones, Hideo Wada and Douglas Wiens, *Diophantine representation of the set of prime numbers*, Vol. 83, No. 6 (Jun.-Jul. 1976), pp. 449-464

[13] J.P. Jones and Y.V. Matiyasevich, *Proof of Recursive Unsolvability of Hilbert's Tenth Problem*, 1991

[14] Yuri V Matiyasevich, Book: *Hilbert's Tenth Problem*, 1993

[15] Daniel Shanks and Samuel S. Wagstaff, Jr., *48 More Solutions of Martin Davis's Quaternary Quartic Equation*, Mathematics of Computation, Vol 64, No. 212, 1995, page 1717-1713

[16] Frans Keune, *www.math.ru.nl/ -keune/Getallen/Getallen.xht#Getallense78.xht (Dutch site)*, 2010

[17] Yuri V Matiyasevich, *Towards Finit-Fold Diophantine Representations*, 2010

[18] Frits Beukers, *Course bundle: Elementary Number Theory*, 2012