LE MATEMATICHE
Vol. LXXIX (2024) – Issue II, pp. 585–620
doi: 10.4418/2024.79.2.18

ON DIOPHANTINE SINGLEFOLD SPECIFICATIONS

D. CANTONE - L. CUZZIOL - E. G. OMODEO

To the memory of Martin
(March 8, 1928 – January 1, 2023)

Consider an $(m+1)$-ary relation $\mathcal{R}$ over the set $\mathbb{N}$ of natural numbers. Does there exist an arithmetical formula $\varphi(a_0,\ldots,a_m,x_1,\ldots,x_\kappa)$, not involving universal quantifiers, negation, or implication, such that the representation and univocity conditions, viz.,

$$\mathcal{R}(\vec{\boldsymbol{a}}) \quad \Longleftrightarrow \quad \exists x_1 \cdots \exists x_\kappa \; \varphi(\vec{\boldsymbol{a}},x_1,\ldots,x_\kappa) \quad \text{and}$$

$$\exists x_1 \cdots \exists x_\kappa \forall y_1 \cdots \forall y_\kappa \left[\varphi(\vec{\boldsymbol{a}},y_1,\ldots,y_\kappa) \implies \&_{i=1}^{\kappa}\big(y_i = x_i\big) \right],$$

are met by each tuple $\vec{\boldsymbol{a}} = \langle \boldsymbol{a}_0,\ldots,\boldsymbol{a}_m \rangle \in \mathbb{N}^{m+1}$?

Even if solely addition and multiplication operators (along with the equality relator and with positive integer constants) are adopted as primitive symbols of the arithmetical signature, the graph $\mathcal{R}$ of any primitive recursive function is representable; but can representability be reconciled with univocity without calling into play one extra operation, namely $\langle b\,,\,n\rangle \mapsto b^n$ (maybe with a fixed integer value > 1 for b)? As a preparatory step toward a hoped-for positive answer to this issue, one may consider replacing the exponentiation operator by any exponential-growth relation.

We discuss the said univocity, aka 'singlefold-ness', issue—first raised by Yuri Matiyasevich in 1974—, framing it in historical context. Moreover, we spotlight eight exponential-growth relation any of which, if Diophantine, could supersede exponentiation in our quest.

Received on September 30, 2024

AMS 2010 Subject Classification: 03D25, 03D35, 11D25, 11D61, 11D72

Keywords: Hilbert's 10th problem, exponential-growth relation, singlefold/finitefold Diophantine representation, rule-them-all equation, Pell's equation, Heegner number.

Acknowledgments: The authors gratefully acknowledge partial support from project "STORAGE–Università degli Studi di Catania, Piano della Ricerca 2020/2022, Linea di intervento 2", from INdAM–GNCS 2019 and 2020 research funds, and from ICSC–Centro Nazionale di Ricerca in High-Performance Computing, Big Data and Quantum Computing.

Contents

1. Introduction

The notions of being listable, exponential Diophantine, and polynomial Diophantine were proved, in the decade 1960/1970, to capture the same family of relations on the set $\mathbb{N}$ of natural numbers (see [13, 23]). Listability had been characterized mathematically decades earlier in various equivalent manners (we will recall one in Sec. 4); the other two notions can be characterized through arithmetical formulae concerning $\mathbb{N}$. To be specific, consider an arithmetic that offers: constants denoting $0,1,2$ and maybe other positive integers; variables ranging over $\mathbb{N}$; operators designating addition, multiplication, and exponentiation; the equality relator. Then:

Definition 1. A relation $\mathcal{D} \subseteq \mathbb{N}^{m+1}$ on natural numbers is said to be [POLYNOMIAL] DIOPHANTINE if there are arithmetical terms D' and D'' involving variables $a_0,\ldots,a_m,x_1,\ldots,x_\kappa$, constants, addition and multiplication, such that[1]

$$\langle \boldsymbol{a}_0,\boldsymbol{a}_1,\ldots \boldsymbol{a}_m\rangle \in \mathcal{D} \quad \Longleftrightarrow \quad \exists x_1 \cdots \exists x_\kappa \, D'(\boldsymbol{a}_0,\boldsymbol{a}_1,\ldots,\boldsymbol{a}_m,x_1,\ldots,x_\kappa) = \\ D''(\boldsymbol{a}_0,\boldsymbol{a}_1,\ldots,\boldsymbol{a}_m,x_1,\ldots,x_\kappa)$$

holds for all $\boldsymbol{a}_0,\boldsymbol{a}_1,\ldots,\boldsymbol{a}_m$ in $\mathbb{N}$. If exponentiation—with variables in the exponent—is also admitted into $D' = D''$, then $\mathcal{D}$ is called EXPONENTIAL DIOPHANTINE.

A function f from $\mathbb{N}^m$ to $\mathbb{N}$ is termed likewise if its GRAPH, namely the relation $\{\langle a_1,\ldots,a_m,\, a_0\rangle \, : f(a_1,\ldots,a_m) = a_0\}$ is Diophantine or, resp., exponential Diophantine. ⊣

A valid biimplication of the form just shown is called a *Diophantine representation* (resp., an *exponential Diophantine representation*) of $\mathcal{D}$. Any listable relation admits an exponential Diophantine representation, as was first proved in [13]: this celebrated result, known as the Davis-Putnam-Robinson (or just *DPR*) theorem, underwent two improvements with respect to its original statement, which we will now recall. In [7], Martin Davis managed to bring exponential specifications to the more generic format[2]

$$\vec{\boldsymbol{a}} \in \mathcal{D} \quad \Longleftrightarrow \quad \exists u \exists v \exists \vec{x} \, [D(\vec{\boldsymbol{a}},\vec{x},u) = 0 \;\&\; \mathscr{J}(u\,,\,v)]\,,$$

where D is a polynomial (multivariate, with coefficients in $\mathbb{Z}$), hence devoid of exponentiation, while exponentiation is superseded by any fixed EXPONENTIAL-GROWTH RELATION (a notion that Julia Robinson proposed in [30] and slightly improved in [31]), i.e., a relation $\mathscr{J}$ such that

[1] Bold symbols often differentiate, henceforth, actual from formal parameters; to wit, values from variables.

[2] Here and below, $\vec{\boldsymbol{a}}$ and $\vec{x}$ shorten $\boldsymbol{a}_0,\boldsymbol{a}_1,\ldots,\boldsymbol{a}_m$ and $x_1,\ldots,x_\kappa$, respectively.

$$\begin{array}{r} \forall u \forall v \big[\, \mathscr{J}(u\,,v) \quad \Longrightarrow \quad v \leqslant u^u \;\;\&\;\; u > 1 \,\big] \quad \text{and} \\ \forall \ell \, \exists u \, \exists v \big[\, \mathscr{J}(u\,,v) \quad \& \quad u^\ell < v \,\big]\,. \end{array} \tag{$\dagger$}$$

In [24], Yuri V. Matiyasevich managed to bring exponential representations to the format[3]

$$\vec{\boldsymbol{a}} \in \mathcal{D} \quad \Longleftrightarrow \quad \exists u \, \exists v \, \exists \vec{x} \, [D(\vec{\boldsymbol{a}}, \vec{x}, u) = 0 \;\&\; 2^u = v]\,,$$

where D is a polynomial, while ensuring singlefold-ness, henceforth dubbed UNIVOCITY, that is: for any $\vec{\boldsymbol{a}}$, *there is at most one solution to the constraint* $D(\vec{\boldsymbol{a}}, \vec{x}, u) = 0 \;\&\; 2^u = v$.

Now and then our focus will zoom in on FINITEFOLD specifications, which are the ones admitting at most a finite number of solutions for each tuple $\vec{\boldsymbol{a}}$ of actual parameters.

Examples of exponential-growth relations are:

$$\mathscr{E}_1 = \big\{ \langle u\,, 2^u \rangle \, : u \in \mathbb{N} \setminus \{0,1\} \big\} \quad \text{and} \quad \mathscr{E}_2 = \big\{ \langle u\,, F_{2u} \rangle \, : u \in \mathbb{N} \setminus \{0,1\} \big\}\,,$$

where F is the Fibonacci progression defined by the recurrence $F_0 = 0\,, F_1 = 1\,,$ and $F_{i+2} = F_i + F_{i+1}$ for $i \in \mathbb{N}$. The relation $\mathscr{E}_1$ suggests the feasibility of an amalgamation—nowhere described in the literature, as far as the authors know—between the cited results of [7] and [24]; as for $\mathscr{E}_2$, it was precisely by exhibiting a polynomial Diophantine representation of it that Matiyasevich revealed the existence of an alike representation of exponentiation itself [23]. Aiming at unearthing the sought amalgamation, we will closely examine (see Sec. 6) Davis' and Matiyasevich's said reductions.

Polynomial Diophantine univocity—or, at worse, finitefold-ness—is the true challenge; this is why we also seek a relation that can play, in this respect, a role analogous to $\mathscr{E}_2$: a relation $\mathscr{M}$ that, in addition to satisfying exponential growth, as well as any other requirements that might emerge from the amalgamated theorem (a potential such requirement is tagged (‡) in Sec. 7), admits a finitefold, hopefully univocal, polynomial specification. After a suggestion provided by [11] (and then reiterated in [22, 27]), in Sec. 8 we candidate for such a role eight relations associated with eight special quaternary quartic equations, at least one of which we should prove to have only finitely many solutions—which, quite regrettably, we have been unable to do so far.

---

[3] Or to the even more elegant one $\vec{\boldsymbol{a}} \in \mathcal{D} \Longleftrightarrow \exists u \, \exists \vec{x} \, [D(\vec{\boldsymbol{a}}, \vec{x}) = 4^u + u]$, cf. [1, pp. 137–138].

The paper is organized as follows. Sec. 2 illustrates, through a gallery of short examples, which kind of relations on $\mathbb{N}$ can be represented univocally by means of Diophantine polynomials without resorting to overly sophisticated tools. It is contended that when univocity does not come for free, it can be built into such a representation by insertion of clauses that insist on the minimality of the values to be assigned to the "unknowns" $x_1, \dots, x_\kappa$; minimality can be enforced by means of bounded universal quantifiers, but can these quantifiers be recast just in terms of addition, multiplication, and existential quantification? Sec. 3 shows that a number-theoretic construct somehow related to bounded universal quantification does, in fact, admit a univocal *exponential* Diophantine representation: the construct we are referring to is the function $p(a,b,c) = \prod_{k=1}^{c}(a+b\cdot k)$, and clues about its kinship to bounded universal quantification are deferred to a later section. Sec. 4 digresses into presenting a special format, known as the *Davis normal form*, that can be used to represent the graph of any primitive recursive function. This is, in essence, a technique for specifying any listable relation in a manner that seemingly deviates from a Diophantine representation, as it involves one bounded universal quantifier. Sec. 4 also recaps a variant of the Davis normal form, enforcing univocity, derived by Yu. Matiyasevich from his momentous finding that every listable relation is Diophantine. All prerequisites are ripe enabling us to produce, in Sec. 5, a univocal exponential representation of any Diophantine—hence of any listable—relation $\mathcal{D}$, through reduction of the bounded universal quantifier to the said construct $p(a,b,c)$. At this point one of Matiyasevich's variants, embodying univocity, of the DPR theorem has been reached; in Sec. 6 we recall a more refined one, in which exponentiation is relegated, within a representation of $\mathcal{D}$, into a single literal of the form $2^u = v$. Two questions are then raised in Sec. 7: Could a suitable condition $\mathscr{M}(u,v)$ supersede this literal in the general representation scheme? And also: Can we manage to place a finitefold Diophantine relation $\mathscr{M}(u,v)$ in this role? The truly original part of this paper is Sec. 8, where we review the entire catalog of our candidate $\mathscr{M}$'s, each one of which is associated with one of the square-free rational integers $d > 1$ such that the algebraic integers of the field $\mathbb{Q}(\sqrt{-d})$ form a unique-factorization domain.

2. Sampler of univocal (or nearly so) Diophantine specifications

Let us start with motivating examples of univocal (polynomial first, then exponential) Diophantine specifications of various relations over $\mathbb{N}$. Before doing so, we observe that Diophantine relations can safely be nested one inside another; moreover, we can unconditionally admit the conjunction connective '$\&$' in the specification language, in view of the equivalences

$$\begin{aligned}
&\big[\exists\vec{x}\;\, P'(\vec{a},\vec{x}) = P''(\vec{a},\vec{x})\big] \;\&\; \big[\exists\vec{y}\;\, Q'(\vec{b},\vec{y}) = Q''(\vec{b},\vec{y})\big] \quad\Longleftrightarrow\\
&\qquad\qquad \exists\vec{x}\,\exists\vec{y}\,\Big[\big(P'(\vec{a},\vec{x}) - P''(\vec{a},\vec{x})\big)^2 + \big(Q'(\vec{b},\vec{y}) - Q''(\vec{b},\vec{y})\big)^2 = 0\Big],\\
&(s-t)^2 + (u-v)^2 = 0 \quad\Longleftrightarrow\quad s^2+t^2+u^2+v^2 = 2\,(s\,t+u\,v)\,,
\end{aligned}$$

which yield

$$\begin{aligned}
&\big[\exists\vec{x}\;\, P'(\vec{a},\vec{x}) = P''(\vec{a},\vec{x})\big] \;\&\; \big[\exists\vec{y}\;\, Q'(\vec{b},\vec{y}) = Q''(\vec{b},\vec{y})\big] \quad\Longleftrightarrow\\
&\qquad\qquad \exists\vec{x}\,\exists\vec{y}\,\big[P'(\vec{a},\vec{x})^2 + P''(\vec{a},\vec{x})^2 + Q'(\vec{b},\vec{y})^2 + Q''(\vec{b},\vec{y})^2 =\\
&\qquad\qquad\qquad 2\cdot\big(P'(\vec{a},\vec{x})\cdot P''(\vec{a},\vec{x}) + Q'(\vec{b},\vec{y})\cdot Q''(\vec{b},\vec{y})\big)\big].
\end{aligned}$$

While these broadenings of the specification language do not affect univocity, the disjunction connective can be brought into play, but should be handled with care: simple-minded use of the rewriting rule $P' = P'' \;\vee\; Q' = Q'' \rightsquigarrow P'\cdot Q' + P''\cdot Q'' = P' \;\cdot Q'' + P''\cdot Q'$ might, in fact, imperil univocity. E.g., restating $a = 0 \vee \exists x\, b = x+1$ as $\exists x\; a\cdot b = a\cdot(x+1)$ would not work, since x could take any value in $\mathbb{N}$ when $a = 0$; this violation of univocity can easily be cured, though: we can overload the first disjunct with the condition $x = 0$ before eliminating propositional connectives, thus getting $\exists x\;(a+x)\cdot b = (a+x)\cdot(x+1)$ via the equivalence $a^2+x^2 = 0 \iff a+x = 0$.

Using ‘:=’ to mean “stands for”, we now provide the specifications of some basic relations among which divisibility, ‘|’, coprimality, ‘⊥’, and the graphs of integer quotient ‘÷’ and remainder operation ‘%’:

$$\begin{array}{rcl@{\qquad}rcl}
a\in\varnothing & := & a = a+1\,; & a\in\{b_0,\dots,b_\ell\} & := & \bigvee_{i\leqslant\ell}\, a = b_i\,;\\
a\leqslant b & := & \exists x\, a+x = b\,; & a<b & := & a+1\leqslant b\,;\\
a\neq b & := & 2\cdot a\cdot b < a^2+b^2\,; & q=\square & := & \exists x\, x^2 = q\,;\\
d\neq\square & := & \exists x\,(x^2<d \;\&\; d\leqslant x^2+2\cdot x)\,; & & & \\
b_1 \max b_2 = a & := & a\in\{b_1,b_2\} \;\&\; b_1\leqslant a \;\&\; b_2\leqslant a\,; & & & \\
b\div a = q & := & \exists r\,\big(a\cdot q+r = b \;\&\; r<a\big)\,; & & & \\
b\,\%\,a = r & := & \exists q\,\big(a\cdot q+r = b \;\&\; r<a\big)\,; & & & \\
a\perp b & := & \exists x_1\,\exists x_2\,\exists y_1\,\exists y_2\,\big(x_1\cdot a+y_1\cdot b = x_2\cdot a+y_2\cdot b+1\big)\,; & & & \\
a\nmid b & := & \exists q\exists r\,\big(a\cdot q+r+1 = b \;\&\; r+1<a\big)\,; & & & \\
a\mid b & := & \exists q\; a\cdot q = b\,; & s\equiv r \mod p & := & p^2\mid(s-r)^2\,;\\
\gcd(a,b) = g & := & g\mid a \;\&\; g\mid b \;\&\; (a\div g)\perp(b\div g). & & &
\end{array}$$

Among these, the specifications lacking univocity are the ones of ‘⊥’, of ‘|’ (insofar as $a\cdot q = b$ holds for any q when $a = b = 0$), and, consequently, of ‘mod’ and ‘gcd’. To fix them, put:

$$\begin{aligned}
a\perp b \;&:=\; \exists x\exists y\exists z\,\big[x^2\cdot a^2+1 = y^2\cdot b^2+2\cdot x\cdot a \;\&\\
&\qquad\qquad\qquad \big(a+b = 1 = x+y+z \;\vee\; x+z+1 = b\big)\big]\,;\\
a\mid b \;&:=\; \exists q\exists z\,\big(a+b+q+z\big)\cdot\big((a\cdot q-b)^2+(z+1-a)^2\big) = 0\,.
\end{aligned}$$

The former states that, unless $a=1 \;\&\; b=0$, the equation $x\,a \pm y\,b = 1$ has a solution (necessarily unique) such that $x<b$; the definiens of the latter states that $(a=b=q=0) \vee (a>0 \;\&\; a\cdot q=b)$ holds for some q.

Likewise, since the specification $\mathsf{Fib}(f) \;:=\; \exists x\, f^2 - x\cdot f - x^2 = \pm 1$ of the property of being a component of the Fibonacci progression (cf. [18, p. 85]) has multiple solutions for $f=1$, we thus transform it into a univocal representation:

$$\mathsf{Fib}(f) \;:=\; \exists x\, \big(f^2-(x+1)\cdot f-(x+1)^2\big)^2 = 1\,.$$

Generally speaking, univocity can be enforced in an existential definition that lacks it by insisting on the minimality of the values assigned to the existential variables, but this brings into play bounded universal quantifiers;[4] and it is far from obvious (see Sec. 5 below) how these can be disempowered into arithmetical constructs. As an illustration of this point, consider the following Diophantine specification (alternative to the one proposed above) of the property of not being a perfect square:

$$d \neq \square \;:=\; \exists x \exists y \exists z \left[x^2 = d\cdot(y+1)^2+1 \;\&\; d=z+1\right].$$

The theory of Pell equations (see, e.g., [28, Sec. 3.4]) ensures the correctness of this characterization; however, the number of solving triples is infinite for each non-square number and it is daredevil to introduce univocity by reformulating the definiens as

$$\begin{array}{ll}\exists x \exists y \exists z\,[& x^2 = d\cdot(y+1)^2+1 \;\&\; d=z+1 \;\& \\ & \forall x' < x \forall y' < y\, \left(x'^2 \neq d\cdot(y'+1)^2+1\right) \quad].\end{array}$$

Remark 1 (Putnam's format of a Diophantine representation)**.** To each univocal Diophantine representation

$$\mathcal{D}(\boldsymbol{a}) \iff \exists \vec{x}\, D(\boldsymbol{a},\vec{x}) = 0$$

of a property of natural numbers, where D is a polynomial with coefficients in $\mathbb{Z}$, there corresponds the following univocal representation of the same property:

$$\mathcal{D}(\boldsymbol{a}) \iff \exists x_0\, \exists \vec{x}\left[(x_0+1)\cdot\big(1-D^2(x_0,\vec{x})\big) = \boldsymbol{a}+1\right]. \qquad \dashv$$

3. Sampler of univocal exponential Diophantine specifications

Suppose now that the only operators adopted as primitive arithmetical constructs are the exponentiation operator, along with a symbol designating the integer value 2. Then addition and multiplication can be viewed as derived constructs

[4] Bounded quantifiers can be introduced as usual; in particular:
$$\forall v \leqslant w\; \varphi \;:=\; \forall v\,(v \leqslant w \Longrightarrow \varphi) \text{ and } \exists v \leqslant w\, \varphi \;:=\; \exists v\,(v \leqslant w \;\&\; \varphi).$$

and no other constant m is essential (since $m = 1 + \cdots + 1$), as the following univocal exponential Diophantine specifications make evident:

$$\begin{array}{rrcl}
 & a=0 & := & \exists t\,\exists u\,\big(u^a = t \;\&\; 2^t = u\big)\,; \\
 & a=1 & := & \exists v\,\big(v=0 \;\&\; 2^v = a\big)\,, \\
\text{i.e.,} & a=1 & := & \exists t\,\exists u\,\exists v\,\big(u^v = t \;\&\; 2^t = u \;\&\; 2^v = a\big)\,; \\
 & a\cdot b=c & := & \exists x\,\exists y\,\big(2^a = x \;\&\; 2^c = y \;\&\; x^b = y\big)\,; \\
 & a+b=c & := & \exists u\,\exists v\,\exists w\,\big(2^a = u \;\&\; 2^b = v \;\&\; 2^c = w \;\&\; u\cdot v = w\big)\,, \\
\text{i.e.,} & a+b=c & := & \exists u\,\exists v\,\exists w\,\exists x\,\exists y\,\big(2^a = u \;\&\; 2^b = v \;\&\; 2^c = w \;\&\; \\
 & & & \qquad\qquad 2^u = x \;\&\; 2^w = y \;\&\; x^v = y\big)\,.
\end{array}$$

It is an easy task to figure out from the above table the following fact, that states more explicitly—and enhances with univocity—what is observed in [13, p. 427]:

Lemma 3.1. *Any exponential Diophantine specification* $\exists x_1 \cdots \exists x_\kappa$ $\varphi(a_0, a_1, \ldots, a_m, x_1, \ldots, x_\kappa)$ *whose matrix* φ *is devoid of quantifiers and only involves the logical connectives* $=$, $\&$, $\vee$ *can be recast as*

$$\exists x_1 \cdots \exists x_\kappa\, \exists y_0\, \exists y_1 \cdots \exists y_\ell \left[y_0 = 2 \;\&\; \&_{i \leqslant s}\, b_i^{n_i} = c_i \right],$$

where: $b_0, b_1, \ldots, b_s$, $n_0, n_1, \ldots, n_s$, $c_0, c_1, \ldots, c_s$ *are variables drawn from the set* $\{a_0, \ldots, a_m, x_1, \ldots, x_\kappa, y_0, \ldots, y_\ell\}$, *and* b_i, n_i, c_i *are distinct signs for each* i.

If the source specification is univocal, so is the "flattened" one resulting from this recasting. $\dashv$

Very early on [30, pp. 446–447], J. Robinson noted that binomial coefficient and factorial function are existentially definable in terms of exponentiation. The following univocal specifications are reminiscent of hers, but we rely, as for the factorial, on the modernized variant provided in [28, pp. 145–146]. The classical binomial theorem and the identities $\binom{\ell}{\ell-i} = \binom{\ell}{i}$, for all $i = 0, 1, \ldots, \ell$, justify the first specification recalled here:

$$\begin{array}{rcl}
\dbinom{\ell}{i} = a & := & \exists u \left[a = \big((u+1)^\ell \div u^i \big) \,\%\, u \;\&\; u = 2^\ell + 1 \right]; \\
j\,! = a & := & a = \left[\big((2\,j)^j \big)^j \div \dbinom{(2\,j)^j}{j} \right].
\end{array}$$

Constructs more general than $c!$ are the *falling factorial* $\prod_{k<c}(a-k)$ with $a \geqslant c$, and the related *raising factorial* $\prod_{k=1}^{c}(a+k)$. Concerning an even more general construct, we have:

Lemma 3.2 (Originating from [12, Lemma 2.2])**.**
Given a, b, c, d, the relationship

$$\prod_{k=1}^{c}(a+b\cdot k) \quad = \quad d$$

*holds if and only if there exist—***and are uniquely determined***—m, p, q, r, s, t such that*

$$\Big(b\cdot c=0 \;\&\; d=a^c \;\&\; m=p=q=r=s=t=0\Big) \vee \Big[b\cdot c=t+1 \;\&\; m=b\cdot(a+b\cdot c)^c+1 \;\&\; b\cdot q=a+m\cdot p \;\&\; \big[b^c\cdot c!\,\tbinom{q+c}{c}\big]\,\%\,m=d \;\&\; \big[(q+r+1=m \;\&\; s=0) \vee (q=m+r \;\&\; p+s+1=b)\big]\Big].$$

Proof. The first disjunct, regarding the case $b=0 \vee c=0$, does not deserve explanation; the second refines the existential specification of $\prod_{k=1}^{c}(a+b\,k)$,

$$\exists m\exists q\exists p\left(m=b\,(a+b\,c)^c+1 \;\&\; b\,q=a+m\,p \;\&\; \left[b^c\,c!\binom{q+c}{c}\right]\%\,m=d\right),$$

proved in [28, pp. 147–149] for the case $b>0 \;\&\; c>0$. That specification leaves p and q under-determined; we are now ensuring univocity by indicating that if one tried to assign a smaller value to q, then either the value of q itself or the corresponding value of p would turn out to be negative. ⊣

A theorem by Éduard Lucas (cf. [15]) enables us to univocally represent, through the binomial coefficient, various *comparing relators and bitwise operations* involving two numbers a and b whose base-2 representations are

$$a \;=\; \textstyle\sum_{i=0}^{k} a_i\,2^i, \qquad b \;=\; \sum_{i=0}^{k} b_i\,2^i, \qquad \textit{where}$$

$$a_i, b_i \in \{0,1\} \qquad \textit{for} \quad i=0,1,\ldots,k.$$

Let us so define MASKING, ORTHOGONALITY, and BITWISE PRODUCT:

$$\begin{array}{ccccccc} a & \sqsubseteq & b & \iff & a_i \leqslant b_i & \textit{for} & i=0,\ldots,k; \\ a & \perp\!\!\!\perp & b & \iff & a_i b_i = 0 & \textit{for} & i=0,\ldots,k; \\ a & \sqcap & b & = & \sum_{i=0}^{k}(a_i\cdot b_i)\cdot 2^i. & & \end{array}$$

After [21, p. 228], we can specify:

$$\begin{array}{llll} a \;\sqsubseteq\; b & := & \exists x \;\binom{b}{a} \;=\; 2\cdot x+1; \\ a \;\perp\!\!\!\perp\; b & := & a \;\sqsubseteq\; a+b; \\ a\sqcap b=c & := & c\sqsubseteq a \;\&\; c\sqsubseteq b \;\&\; a-c \perp\!\!\!\perp b-c. \end{array}$$

In Sec. 4, we will exploit three computable functions admitting univocal exponential specifications; they are an injection from $\mathbb{N}^2$ onto $\mathbb{N}$ and its associated projections (see [14, Sec. 3.8]):

$$\begin{array}{rcrcl} \varpi(a,b)=c & := & 2^a(2b+1) & = & c+1\,; \\ \lambda(c)=a & := & 2^a \mid c+1 & \& & 2^{a+1} \nmid c+1\,; \\ \rho(c)=b & := & \exists x\ \ 2^x(2b+1) & = & c+1\,. \end{array}$$

These definitions yield, for all $a,b,c,a',b' \in \mathbb{N}$, that:

$$\begin{array}{rcl} \varpi(a,b)=c & \iff & \lambda(c)=a \ \& \ \rho(c)=b\,, \\ a<a' \ \& \ b<b' & \Longrightarrow & \varpi(a,b)<\varpi(a',b) \ \& \ \varpi(a,b)<\varpi(a,b')\,. \end{array}$$

4. Listable sets and the Davis normal form

Intuitively speaking, a set $\mathscr{R} \subseteq \mathbb{N}^{m+1}$ is *listable* if there is an effective procedure for making a list (with repetition allowed) of the elements of $\mathscr{R}$. Computability theory provides the notion of a RECURSIVELY ENUMERABLE (R.E.) set as the formal counterpart—adequate, according to the Church–Turing thesis—of this intuitive notion. One of several equivalent ways to characterize it is:[5]

Characterization 1. An $(m+1)$-ary relation $\mathscr{R}$ on $\mathbb{N}$ is called R.E. if either $\mathscr{R}=\emptyset$ or there are *primitive recursive* functions $r_0,r_1,\ldots,r_m$ from $\mathbb{N}$ to $\mathbb{N}$ such that

$$\mathscr{R} \ = \ \{\langle r_0(i),r_1(i),\ldots,r_m(i)\rangle \ : i \in \mathbb{N}\}\,.$$

As this definition suggests, we mainly refer to monadic functions henceforth; hence we can rely on an *ad hoc* characterization of primitive recursiveness, that we borrow from [14, Sec. 4.9]:

Characterization 2. Put $\mathtt{n}(x)=0$ and $\mathtt{s}(x)=x+1$ for each $x \in \mathbb{N}$. PRIMITIVE RECURSIVE FUNCTIONS are all and only those functions from $\mathbb{N}$ to $\mathbb{N}$ that either belong to the initial endowment $\mathtt{n}(\centerdot)$, $\mathtt{s}(\centerdot)$, and $\lambda(\centerdot)$, $\rho(\centerdot)$ (see above, end of Sec. 3), or are obtainable from that endowment through repeated use of the following three operations:

1. *composing* $f(\centerdot)$ and $g(\centerdot)$ into the function $f \circ g$ that sends every x to $f\big(g(x)\big)$;
2. *pairing* $f(\centerdot)$ and $g(\centerdot)$ into the function $f \otimes g$ that sends every x to $\varpi\big(f(x),g(x)\big)$ (see above);

[5] In Sec. 8, another characterization of r.e. sets will underlie clause *i)* of (¶).

3. obtaining by *recursion* from $f(\centerdot)$ and $g(\centerdot)$ the function

$$h(x) \quad := \quad \begin{cases} 0 & \text{if} \quad x = 0\,, \\ f\,(x \div 2) & \text{if} \quad x \in \{1,3,5,7,\dots\}\,, \\ g\,(h\,(x \div 2)) & \text{if} \quad x \in \{2,4,6,8,\dots\}\,. \end{cases}$$

We then have:

Theorem 1. The graph

$$\mathcal{F}(a,b) \quad \Longleftrightarrow \quad F(a) = b$$

of any primitive recursive function F from $\mathbb{N}$ into $\mathbb{N}$ can be specified by means of an arithmetical formula φ within which all universal quantifiers are bounded and negation does not occur *(nor does implication; usage of the conjunction and disjunction connectives* $\&$, $\vee$ *is subject to no restraints; also existential quantification can be used with no restraints, because we are assuming as a primitive sign* $\exists$ *on a par with* $\forall$*).*

Proof. The graphs of the initial functions $\mathtt{n}(\centerdot)$, $\mathtt{s}(\centerdot)$, $\lambda(\centerdot)$, and $\rho(\centerdot)$ can be specified, respectively, by $a+b=a$, $a+1=b$, $\exists p\, \exists x\big(Pow(b,p)\ \&\ p\cdot(2x+1) = a+1\big)$, and $\exists x\, \exists p\big(Pow(x,p)\ \&\ p\cdot(2b+1) = a+1\big)$, where $Pow\,(a,b)$ is a formula describing the graph of 2^a—this function gets the value 1 when $a=0$ and gets the value $2\cdot 2^t$ when $a=t+1$. By exploiting the Chinese remainder theorem in the manner explained in [31, pp. 79–80],[6] we get the specification

$$\begin{aligned} Pow\,(a,b) \quad := \quad \exists u \exists d \Big[\quad & 1 = u \,\%\, \big(1+d\big)\ \&\ b = u \,\%\, \big(1+(a+1)\cdot d\big)\ \& \\ & \forall t \leqslant a\Big(\, u \,\%\, \big(1+(t+2)\cdot d\big) \ = \\ & \qquad 2\cdot \big[u \,\%\, \big(1+(t+1)\cdot d\big)\big]\, \Big)\Big]\,. \end{aligned}$$

As for the mechanisms enabling the immediate construction of primitive recursive functions out of $f(\centerdot)$ and $g(\centerdot)$ that are supposed to satisfy the induction hypothesis, we so specify the

graph of $f \circ g$: $\quad \exists y\big(g(a) = y\ \&\ f(y) = b\big)$,

graph of $f \otimes g$: $\quad \begin{cases} \exists x \exists y \exists p\Big[\quad f(a) = x\ \&\ g(a) = y\ \& \\ \qquad\qquad Pow(x,p)\ \&\ p\cdot(y+y+1) = b+1\Big]\,, \end{cases}$

[6] A corollary, originating from Gödel (1931), of the Chinese remainder theorem says: Consider integers $a_0,\dots,a_n$ such that $0 \leqslant a_i < q$ holds for each i, and put $q_i \ = \ 1+n!\cdot q\cdot(i+1)$. Then $a_0 = a \,\%\, q_0,\dots,a_n = a \,\%\, q_n$ hold together for a sole $a < \prod_{j\leqslant n} q_j$.

and then conclude by so specifying the outcome of recursion:

$$\begin{array}{l}\exists u \exists d \exists m\Big[\;\; 0 = u \,\%\, \big(1+d\big) \;\;\&\;\; b = u \,\%\, \big(1+(a+1)\cdot d\big) \;\;\&\;\; m = a \div 2 \;\;\& \\ \qquad\qquad \forall t \leqslant m\Big(\; f(t) = u \,\%\, \big(1+(2\cdot t+2)\cdot d\big) \;\;\& \\ \qquad\qquad\qquad\qquad g\big(u \,\%\, \big(1+(t+2)\cdot d\big)\big) = u \,\%\, \big(1+(2\cdot t+3)\cdot d\big) \;\Big)\Big].\end{array}$$

Needless to say, here the Chinese remainder theorem is at work again. ⊣

In light of the elicitation Char. 1 of listability, Thm. 1 can easily be generalized into:

Theorem 2. Every listable (property or) relation on $\mathbb{N}$ can be specified by means of an arithmetical formula wherein all universal quantifiers are bounded and neither negation nor implication occurs. ⊣

In [31, pp. 93–96], a syntactic manipulation algorithm is described that transforms any arithmetical formula φ endowed with the features stated in Thm. 1 (and in Thm. 2), and whose free variabes are $a_0, a_1, \dots, a_m$, into a Diophantine polynomial $R(h, y, a_0, \dots, a_m, x_1, \dots, x_\kappa)$ such that:

$$\begin{array}{rcl}\varphi(a_0,\dots,a_m) & \Longleftrightarrow & \exists h\, \forall y \leqslant h\, \exists x_1 \leqslant h \cdots \exists x_\kappa \leqslant h \\ & & \qquad\qquad\qquad \big[R(h,y,a_0,\dots,a_m,x_1,\dots,x_\kappa) = 0\big].\end{array}$$

This special format is called DAVIS NORMAL FORM, because it was first brought to light (originally lacking bounds on the inner existential quantifiers) in [5, Part III]. We will now report on a perfectioning of this format, that Yuri Matiyasevich put forward after establishing that the *a priori* distinct notions of r.e. set and Diophantine set amount to one another (cf. [23]).

Ancillary to that, let us introduce the Cantor functions c_ℓ, with $\ell \in \mathbb{N} \setminus \{0\}$:

$$\begin{array}{rcl}\mathsf{c}_1(u_1) & := & u_1\,, \\ \mathsf{c}_{q+2}(u_1,\dots,u_{q+2}) & := & \mathsf{c}_{q+1}\left(u_1,\dots,u_q, \dfrac{(u_{q+1}+u_{q+2})^2 + 3\cdot u_{q+1} + u_{q+2}}{2}\right).\end{array}$$

(Notice that $(u_{q+1}+u_{q+2})^2 + 3\cdot u_{q+1} + u_{q+2}$ is an even number.) It thus turns out that each c_ℓ is a monotone injection of $\mathbb{N}^\ell$ onto $\mathbb{N}$ (cf. [17]). Yu. Matiyasevich stated:

Lemma 4.1 ([25, pp. 303–304])**.** *To each Diophantine polynomial $D(a_0,\dots,a_m,x_1,\dots,x_\kappa)$, there correspond Diophantine polynomials $P(h,y,a_0,\dots,a_m,x_0,x_1,\dots,x_\kappa) \geqslant 0$ and $E(a_0,\dots,a_m,h) \geqslant 0$ such that* *the following biimplications hold (where $\vec{a}$ and $\vec{x}$ shorten $a_0,\dots,a_m$ and $x_0,x_1,\dots,x_\kappa$, respectively):*[7]

$$\begin{array}{rl}
\exists x_1 \cdots \exists x_\kappa\, D(\vec{a},x_1,\dots,x_\kappa)=0 & \iff \exists h\, \forall y \leqslant h \quad \exists \vec{x} \quad P(h,y,\vec{a},\vec{x})=0 \\
& \iff \exists ! h \ \ \forall y \leqslant h\ \exists \vec{x} \quad P(h,y,\vec{a},\vec{x})=0 \\
& \iff \exists h \ \ \forall y \leqslant h\ \exists ! \vec{x} \quad P(h,y,\vec{a},\vec{x})=0 \\
\multicolumn{2}{r}{\iff \exists h\, \forall y \leqslant h\ \exists x_0 \leqslant E(\vec{a},h)\ \exists x_1 \leqslant E(\vec{a},h) \cdots \exists x_\kappa \leqslant E(\vec{a},h) \quad P(h,y,\vec{a},\vec{x})=0\,.}
\end{array}$$

Proof. We will define $P(h,y,\vec{a},x_0,x_1,\dots,x_\kappa)$ so that $P=0$ enforces univocally (also with respect to the new existential variables, h and x_0) the condition

$$\mathsf{c}_\kappa(x_1,\dots,x_\kappa)=y \quad \& \quad \big[\big(y<h \ \& \ D(\vec{a},x_1,\dots,x_\kappa)\neq 0\big) \quad \vee \\ \big(y=h \ \& \ D(\vec{a},x_1,\dots,x_\kappa)=0\big)\big].$$

For this purpose, we put[8]

$$\begin{array}{rcl}
P & := & 2^{2^\kappa}\cdot\big(y-\mathsf{c}_\kappa(x_1,\dots,x_\kappa)\big)^2 + \\
& & \big[(h-y)\cdot D^2(\vec{a},x_1,\dots,x_\kappa)-x_0-1\big]^2 \cdot \big[(h-y)^2+D^2(\vec{a},x_1,\dots,x_\kappa)+x_0\big].
\end{array}$$

It is then clear that the variables h, $x_1,\dots,x_\kappa$, and x_0 on the right-hand side of the claimed biimplications designate, respectively: the first u such that the κ-tuple $\langle \hat{x}_1,\dots,\hat{x}_\kappa\rangle$ for which $\mathsf{c}_\kappa(\hat{x}_1,\dots,\hat{x}_\kappa)=u$ holds solves the equation $D(\vec{a},x_1,\dots,x_\kappa)=0$ (in the unknowns $x_1,\dots,x_\kappa$); for each $y \leqslant h$, the κ-tuple $\langle x_{y,1},\dots,x_{y,\kappa}\rangle$ such that $\mathsf{c}_\kappa(x_{y,1},\dots,x_{y,\kappa})=y$; the accordance between positivity of $h-y$ and non-nullity of $D(\vec{a},x_{y,1},\dots,x_{y,\kappa})$. When the left-hand side of each claimed biimplication is satisfied by specific a_i's, we can hence determine—and they are unique—a value for h and, corresponding to each y, values $x_{y,j}$'s that do to the case of the right-hand side; conversely, if h satisfies the right-hand side for given a_i's, then the corresponding $x_{h,1},\dots,x_{h,\kappa}$ are such that $D(\vec{a},x_{h,1},\dots,x_{h,\kappa})=0$. To end, we must address the issue of setting a suitable bound $E(\vec{a},h)$ on the variables x_j. Since no $x_{y,j}$ with $j>0$ can exceed h, we will enforce $E(\vec{a},h)\geqslant h$; to also take into proper account the values $x_{y,0}$, we put $E(\vec{a},h) := h\cdot\big(1+\widetilde{E}(\vec{a},h)\big)$, where $\widetilde{E}(\vec{a},h)$ results from the polynomial $D^2(\vec{a},h,\dots,h)$ through replacement of each one of its coefficients, k, by the absolute value $|k|$. ⊣

5. Reducing bounded universal quantifiers to exponentiation

The proof that the family of exponential Diophantine relations is closed under bounded universal quantification can be developed in many different ways (see

[7] The sign '$\exists!$' (read: "there exists a sole") can be introduced as an abbreviation: $\exists!\, v\, \varphi \ := \ \exists u \forall v\, (\varphi \iff v=u)$, where u does not occur in φ and is distinct from v.

[8] The factor 2^{2^κ} abundantly suffices to elide the denominator of the polynomial c_κ.

[26, Chap.6] and [21, pp. 231–232]). Here we resume part of the development (Lemmas 5.1 e 5.2) from the recent monograph [28]—see also [10, pp. 252–256], in turn stemming from [13, pp. 433–435]—; the other part (Lemma 4.1 above and Lemma 5.3 below) is instead adapted from [24], in order to ensure univocity.

Lemma 5.1. (Cf. [28, p. 154]). *To each Diophantine polynomial* $P(h, y, a_1, \dots, a_m, x_1, \dots, x_\kappa)$, *there correspond Diophantine polynomials* $Q(h, u, a_1, \dots, a_m)$ *such that the following hold:*

- $Q(h, u, a_1, \dots, a_m) > h \max u$;
- $Q(h, u, a_1, \dots, a_m) \geqslant |P(h, y, a_1, \dots, a_m, x_1, \dots, x_\kappa)|$ *when* $y \leqslant h$ *and* $x_1, \dots, x_\kappa \leqslant u$.

Proof (just a clue). The trick is similar to the one used at the end of the proof of Lemma 4.1. ⊣

Lemma 5.2 (From [28, pp. 150–153]). *If P and Q are as in Lemma 5.1 then, given* $h, u, a_1, \dots, a_m$,

$$\forall y \leqslant h \, \exists x_1 \leqslant u \cdots \exists x_\kappa \leqslant u \quad P(h, y, a_1, \dots, a_m, x_1, \dots, x_\kappa) \; = \; 0$$

will hold if and only if there exist $t, z, w_1, \dots, w_\kappa$ *such that*

(1) $t = Q(h, u, a_1, \dots, a_m)\,!$;

(2) $1 + (z+1)t = \prod_{y \leqslant h} \big(1 + (y+1)t\big)$;

(3) $P(h, z, a_1, \dots, a_m, w_1, \dots, w_\kappa) \equiv 0 \mod 1 + (z+1)t$;

(4) $1 + (z+1)t \mid \prod_{j \leqslant u}(w_i - j)$, *for* $i = 1, \dots, \kappa$. ⊣

Lemma 5.3. *Out of any given Diophantine polynomial* $D(a_1, \dots, a_m, x_1, \dots, x_\kappa)$, *one can construct three polynomials,* $P(h, y, a_1, \dots, a_m, x_0, x_1, \dots, x_\kappa)$, $E(a_1, \dots, a_m, h)$, *and* $Q(h, u, a_1, \dots, a_m)$, *each producing values in* $\mathbb{N}$ *when its variables range over* $\mathbb{N}$, *such that* $\exists x_1 \cdots \exists x_\kappa \, D(a_1, \dots, a_m, x_1, \dots, x_\kappa) = 0$ *holds if and only if there exist* ***uniquely determined*** $h, u, t, z, w_0, \dots, w_\kappa, g_0, \dots, g_\kappa, f_0, \dots, f_\kappa$, *and e satisfying the following exponential Diophantine conditions:*

(1) $u = E(a_1, \dots, a_m, h) \;\&\; t = Q(h, u, a_1, \dots, a_m)\,!$;

(2) $e = 1 + (z+1)t \;\&\; e = \prod_{y=1}^{h+1} \big(1 + yt\big)$;

(3) $e \mid P(h, z, a_1, \dots, a_m, w_0, w_1, \dots, w_\kappa)$;

(4) $g_i + u = w_i \ \& \ e \mid \prod_{j \leqslant u}\big(g_i + j\big)$, *for* $i = 0, 1, \dots, \kappa$*;*

(5) $\bigvee_{i \leqslant \kappa}\Big[\big(\&_{j<i}\, g_j = f_j + e\big) \ \& \ g_i + f_i + 1 = e \ \& \ \&_{j=i+1}^{\kappa} f_j = 0\Big]$.

Proof. From D—assuming without loss of generality that $m > 0$—we obtain P and E as in Lemma 4.1, then we get Q from P as in Lemma 5.1 (there is but one extra variable, x_0). Now we can apply Lemma 5.2, with $u = E(a_1, \dots, a_m, h)$, and this accounts for the conditions (1)–(4). By means of the g_i, we are requiring that $w_i \geqslant u$; this is a legitimate request, in the light of the proof of Lemma 5.2, whose congruence $P(u, z, a_1, \dots, a_m, w_0, w_1, \dots, w_\kappa) \equiv 0 \mod e$ is rewritten as a divisibility constraint between natural numbers here, by taking the fact $P(h, z, a_1, \dots, a_m, w_0, w_1, \dots, w_\kappa) \geqslant 0$ into account; moreover, within that proof we had represented each $w_i - x_{y,i}$ in the form $w_i - j$ with $0 \leqslant j \leqslant u$, here we are representing it in the form $g_i + j$ with $0 \leqslant j \leqslant u$.

As Lemma 4.1 suggests, in order to make the specification (1)–(4) univocal, it is enough to bring into play new unknowns $f_0, \dots, f_\kappa$ subject to the constraint (5). That is, we are choosing as representative of the infinitely many $(\kappa + 1)$-tuples $\langle w_0, \dots, w_\kappa \rangle$ suitable to encode the list of tuples $\langle x_{0,i}, \dots, x_{h,i} \rangle$ $(i = 0, \dots, \kappa)$ as described within the proof of Lemma 5.2, the one whose components cannot be lowered by the amount e without at least one among them becoming smaller than u. ⊣

Knowing that each listable set has a representation $\exists \vec{x}\, D(\vec{a}, \vec{x}) = 0$, we can view Lemma 5.3 as enriching the DPR theorem [13] with singlefold-ness; in short:

Theorem 3 (Matiyasevich, 1974)**.** Each listable set has a ***univocal*** exponential Diophantine representation. ⊣

6. Exponentiation as a notable quotient

Denote by $\langle \boldsymbol{y}_i(a) \rangle_{i \in \mathbb{N}}$ the endless, strictly ascending sequence consisting of all non-negative integer solutions to the special-form Pell equation[9]

$$(a^2 - 1)\, y^2 + 1 \;=\; \square \quad \text{with} \quad a \in \mathbb{N} \setminus \{0, 1\}\ ;$$

also put $\boldsymbol{x}_i(a) := \sqrt{(a^2 - 1)\boldsymbol{y}_i^2(a) + 1}$. Then:

[9] Once more, '$Q = \square$' means that Q must be a perfect square.

Lemma 6.1. *The following law determines* ***uniquely*** *the values of u, v:*

$$\big((b \geqslant 1 \vee n = 0) \mathbin{\&} a > b^n\big) \implies \left[\begin{array}{l} b^n = c \iff \exists u \exists v \Big(u^2 - (a^2 b^2 - 1)\, v^2 = 1 \mathbin{\&} \\ \qquad \boldsymbol{x}_n(a) \;\leqslant\; u \;<\; a\boldsymbol{x}_n(a) \mathbin{\&} c \;=\; u \div \boldsymbol{x}_n(a)\Big) \end{array}\right].$$

Moreover, if $b \geqslant 1 \mathbin{\&} w \geqslant 3\,(c+1)(n+1)$, then

$$b^n = c \iff c = \boldsymbol{y}_{n+1}(bw+1) \div \boldsymbol{y}_{n+1}(w)\,.$$

Proof. Concerning the first claim, the proof can be traced back to [30, Lemmas 9 and 10] (see also [7, Lemma 3]). Concerning the second claim, see [25, p. 308]. ⊣

Through the first claim of Lemma 6.1, M. Davis obtained an elegant, generalized restatement of the DPR theorem, where a single literal involving an exponential-growth relation $\mathscr{J}$ replaces exponentiation. In addition to $\mathscr{J}(\cdot,\cdot)$, Davis' technique leverages a Diophantine relation $\mathscr{D}(\cdot,\cdot,\cdot)$ on $\mathbb{N}$, such that[10]

- $\forall b \forall n \forall v \forall t \left[v > t \mathbin{\&} \mathscr{D}(b,n,t) \implies v > b^n \right]$ and
- $\forall b \forall n \exists t \;\; \mathscr{D}(b,n,t)$,

along with the Diophantine relation

$$\begin{array}{lll} \mathscr{E}(b,n,c,a,\ell) & := & \exists u \exists v \exists w \big[\; \big(b = u = v = c = 0 \mathbin{\&} n = w+1\big) \vee \\ & & \qquad \big(u^2 - (a^2 b^2 - 1)\, v^2 = 1 \mathbin{\&} w = 0 \mathbin{\&} \\ & & \qquad \;\ell \leqslant u < a\ell \mathbin{\&} c = u \div \ell\big) \qquad \big]. \end{array}$$

It can be shown that

$$\mathop{\&}_{i \leqslant s} b_i^{n_i} = c_i \iff (\exists a, t_0, \ldots, t_s, \ell_0, \ldots, \ell_s) \mathop{\&}_{i \leqslant s} \Big[\mathscr{D}(b_i, n_i, t_i) \mathbin{\&} a > t_i \mathbin{\&} \\ \mathscr{E}(b_i, n_i, c_i, a, \ell_i) \mathbin{\&} \ell_i = \boldsymbol{x}_{n_i}(a) \Big],$$

whence $\boldsymbol{x}_{n_i}(a)$ can be eliminated thanks to the following proposition:

Lemma 6.2 (Cf. [4, Lemma A.2])**.** *Suppose that $a > 1$, $a > n$, and $\boldsymbol{x}_a(a) > \ell$. Then,*

$$\ell = \boldsymbol{x}_n(a) \iff \exists r \;\; \ell^2 - (a^2 - 1)\big(n + (a-1)\,r\big)^2 = 1\,.$$

[10] For definiteness, one could take $\mathscr{D}(b,n,t) := \mathscr{Q}(b+n+2,t)$, where $\mathscr{Q}(w,u)$ is as in [1, p. 155], namely:

$$\mathscr{Q}(w,u) \;:=\; (\exists x, y)\Big[u \geqslant wx \mathbin{\&} x > 1 \mathbin{\&} x^2 - (w^2-1)(w-1)^2 y^2 = 1 \Big].$$

Ultimately, one gets the following proposition, whose proof we omit:

Lemma 6.3. *If $\mathscr{J}(\cdot,\cdot)$ is an exponential-growth relation and each b_i, n_i, c_i is either a variable or a non-negative integer constant, then we have*

$$\begin{aligned}\&_{i\leqslant s}\, b_i^{n_i} = c_i \iff (\exists u, v, t_0,\ldots,t_s, \ell_0,\ldots,\ell_s, r_0,\ldots,r_s)\Big[\, & \mathscr{J}(u,v) \;\&\\ \&_{i\leqslant s}\Big[\, & \mathscr{D}(b_i,n_i,t_i) \;\&\; u>t_i \;\&\; u>n_i \;\&\\ & \mathscr{E}(b_i,n_i,c_i,u,\ell_i) \;\&\; \ell_i<v \;\&\\ & \ell_i^2=(u^2-1)\left[n_i+(u-1)\,r_i\right]^2+1\,\Big]\;\Big].\end{aligned}$$

Therefore, in view of Lemma 3.1:

Theorem 4 (Davis, 1963)**.** Each listable subset of a Cartesian power $\mathbb{N}^{m+1}$ admits a specification of the form $\exists u\,\exists v\,\exists\vec{x}\left[\mathscr{J}(u,v) \;\&\; D(\vec{a},\vec{x},u,v)=0\right]$, where D is a Diophantine polynomial and $\mathscr{J}$ is any exponential-growth relation. ⊣

In one respect, this achieves more than Thm. 3; in fact, here we have a generic exponential-growth relation in place of exponentiation. But, regrettably, univocity is not ensured.

Matiyasevich made a leap towards a reconciliation between Thm. 3 and Thm. 4 in [25, pp. 308–309]. In his theorem, reported below, the specific relation $2^u = v$ occurs instead of a generic $\mathscr{J}(u,v)$; and in its proof (which we omit) the second claim of Lemma 6.1 plays a decisive role:

Theorem 5 (Exponentiation, from dyadic to monadic)**.** A ***univocal*** exponential Diophantine specification of any relation $\&_{i=1}^{s}\, b_i^{n_i} = c_i$ (where b_i, n_i, c_i are as said above) is:

$$\begin{aligned}&\exists u\,\exists v\;\exists e_1\,\exists f_1\,\exists g_1\,\exists h_1\cdots\exists e_s\,\exists f_s\,\exists g_s\,\exists h_s\big[\;\mathcal{L}_1 \;\&\; \mathcal{L}_2 \;\&\\ &\qquad \&_{i=1}^{s}\left[(b_i=0 \;\&\; \mathcal{L}_{3,i}) \vee (b_i>0 \;\&\; \mathcal{L}_{4,i} \;\&\; \mathcal{L}_{5,i} \;\&\; \mathcal{L}_{6,i} \;\&\; \mathcal{L}_{7,i})\right]\big],\end{aligned}$$

where

$$\begin{aligned}\mathcal{L}_1 &:= 2^u=v,\\ \mathcal{L}_2 &:= u=20\textstyle\sum_{i=1}^{s}(c_i+1)(2b_i+1)(n_i^2+1),\\ \mathcal{L}_{3,i} &:= [(n_i=0 \;\&\; c_i=1) \vee (n_i>0 \;\&\; c_i=0)] \;\&\; e_i+f_i+g_i+h_i=0,\\ \mathcal{L}_{4,i} &:= c_i=f_i \div h_i,\\ \mathcal{L}_{5,i} &:= e_i^2-\left((b_i u+1)^2-1\right)f_i^2=1 \;\&\; g_i^2-\left(u^2-1\right)h_i^2=1,\\ \mathcal{L}_{6,i} &:= f_i\equiv n_i+1 \bmod (b_i u) \;\&\; h_i\equiv n_i+1 \bmod (u-1),\\ \mathcal{L}_{7,i} &:= f_i<v \;\&\; h_i<v.\end{aligned}$$

Consequently, every listable subset $\mathcal{R}$ of a Cartesian power $\mathbb{N}^{m+1}$ admits univocal representations $\exists u\,\exists v\,\exists\vec{x}\left[2^u=v \;\&\; D(a_0,\ldots,a_m,\vec{x},u,v)=0\right]$ and

$\exists t\,\exists u\,\exists w\,\exists\vec{x}\Big[\,\big[u+(u+t)^2\big]\cdot\big[1-D^2(a_0,\ldots,a_m\,,\vec{x},\,u,\,u+t)\big]\;=\;4^w+w\Big]$, with D a Diophantine polynomial. ⊣

Remark 2. When $m=0$, the former of the above representations of $\mathcal{R}$ can be reformulated—retaining univocity, and in analogy with Putnam's format seen in Remark 1—as

$$\mathcal{R}(a_0) \quad\Longleftrightarrow\quad \exists x_0\,\exists\vec{x}\,\exists u\,\Big[(x_0+1)\cdot 0^{D^2(x_0,\vec{x},u,2^u)}\;=\;a_0+1\Big]. \qquad ⊣$$

7. Two elusive issues concerning Diophantine finitefold-ness

We are after a generalized variant of Thm. 5 which has, in place of its $2^u=v\ \&\ \mathcal{L}_2\ \&\ \&_{i=1}^{s}[(b_i=0\ \&\ \mathcal{L}_{3,i})\vee(b_i>0\ \&\ \mathcal{L}_{4,i}\ \&\ \mathcal{L}_{5,i}\ \&\ \mathcal{L}_{6,i}\ \&\ \mathcal{L}_{7,i})]$, a suitable formula $\mathscr{M}(u,v)\ \ \&\ \ D(\vec{a},\vec{x},u,v)=0$, where D is a Diophantine polynomial in the parameters $\vec{a}$ and

- $\mathscr{M}$ is a dyadic relation subject to *particular requirements*—probably stronger than exponential growth. Moreover,
- a concrete such $\mathscr{M}$ should be exhibited that admits a *finitefold*—hopefully univocal—Diophantine polynomial specification.

The achievement of these two goals would answer positively an issue raised in [24] and [11]: "OPEN PROBLEM: *Is there a finitefold (or better a singlefold) Diophantine definition of* $a=b^c$ *?*"

As regards which requirement should be imposed on $\mathscr{M}$, [22, p. 749] suggests the following (without explaining, though, why this would be adequate to ensure that the relation $2^u=v$—and therefore any listable set—has a finite Diophantine specification if $\mathscr{M}(u,v)$ has one):

> Integers $\alpha>1$, $\beta\geqslant 0$, $\gamma\geqslant 0$, $\delta>0$ exist such that to each $w\in\mathbb{N}\setminus\{0\}$ there correspond u,v such that: $\mathscr{M}(u,v)$, $u<\gamma w^{\beta}$, and $v>\delta\,\alpha^{w}$ hold. (‡)

As for a concrete choice of $\mathscr{M}$, the most promising candidate at the time when [11] was published was an exponential-growth relation, $\mathscr{M}_7$, associated in a certain manner with the quaternary quartic equation $9\cdot(u^2+7v^2)^2-7\cdot(r^2+7s^2)^2=2$ that had been spotlighted in [8]. The proposed $\mathscr{M}_7$ would admit a finitefold Diophantine polynomial specification if the said equation only had a finite number of integer solutions. Below, we will spotlight a few other quaternary quartics that may candidate as rule-them-all equations.

8. Potential rule-them-all equations: how helpful?

In [8], Martin Davis argued that Hilbert's 10th problem would turn out to be algorithmically unsolvable if his quaternary quartic just recalled could be shown to admit only one solution in $\mathbb{N}$ (an expectation, btw, that came to an end in the early 1970s). In [1, 3, 4], by following Davis' same construction pattern, we increased the number of Diophantine equations that candidate as "rule-them-all equations". Each such equation is associated with one of the eight so-called Heegner numbers $d \neq 1$ (see below): today we know that, if any of the equations associated with the respective Pell equations $x^2 - d\,y^2 = 1$ turned out to admit only a finite number of solutions in $\mathbb{Z}$, then every *listable* subset of $\mathbb{N}^m$—first and foremost the set of all triples $\langle b,n,c\rangle$ such that $b^n = c$—would admit a finitefold polynomial Diophantine representation.

№ d	Associated quaternary quartic equation
2	$2\cdot\left(r^2+2\,s^2\right)^2-\left(u^2+2\,v^2\right)^2 \;=\; 1$
3	$3\cdot\left(r^2+3\,s^2\right)^2-\left(u^2+3\,v^2\right)^2 \;=\; 2$
7	$7\cdot\left(r^2+7\,s^2\right)^2-3^2\cdot\left(u^2+7\,v^2\right)^2 \;=\; -2$
11	$11\cdot\left(r^2+r\,s+3\,s^2\right)^2-\left(v^2+v\,u+3\,u^2\right)^2 \;=\; 2$
19	$19\cdot 3^2\cdot\left(r^2+r\,s+5\,s^2\right)^2-13^2\cdot\left(v^2+v\,u+5\,u^2\right)^2 \;=\; 2$
43	$43\cdot\left(r^2+r\,s+11\,s^2\right)^2-\left(v^2+v\,u+11\,u^2\right)^2 \;=\; 2$
67	$67\cdot 3^6\cdot\left(r^2+r\,s+17\,s^2\right)^2-13^2\cdot\left(v^2+v\,u+17\,u^2\right)^2 \;=\; 2$
163	$163\cdot 3^2\cdot 11^2\cdot 19^2\cdot\left(r^2+r\,s+41\,s^2\right)^2-5^2\cdot\left(v^2+v\,u+41\,u^2\right)^2 \;=\; 2$

This means that to any partially computable function $f(\vec{a})$ from $\mathbb{N}^m$ to $\mathbb{N}$, there would correspond a multi-variate polynomial $D \in \mathbb{Z}[a_1,\ldots,a_m,x_1,\ldots,x_\kappa]$ such that for each $\vec{a} \in \mathbb{N}^m$ the following two conditions (representation and finitefold-ness) hold:

$$\begin{array}{lll} i) & f(\vec{a}) \text{ yields a value} \iff \exists \vec{x} \in \mathbb{N}^\kappa\; D(\vec{a},\vec{x}) = 0\,; & \\ ii) & \exists b \in \mathbb{N}\; \forall \vec{x} \in \mathbb{N}^\kappa\; \left(D(\vec{a},\vec{x}) = 0 \implies b > \sum \vec{x}\right)\,. & \end{array} \qquad (¶)$$

This would be the case if, say, the first of the above-listed quartic equations admitted only the trivial solutions $r = \pm 1$, $s = 0$, $u = \pm 1$, $v = 0$; unfortunately, as will be reported in Sec. 8.6, this is not the case.

Why would it be important to establish whether any of the above equations has only a finite number of solutions? The whole point is that if the equation associated with d is finitefold, then the following dyadic relation $\mathscr{M}_d$ over $\mathbb{N}$

admits a polynomial Diophantine representation:

$d \in \{2,7\}:\quad \mathscr{M}_d(p,q) := \exists \ell > 4 \left[q = \widetilde{\boldsymbol{y}}_{2^\ell}(d)/h_d \;\&\; p \mid q \;\&\; p \geqslant 2^{\ell+1} \right];$

$d \in \{3,11,19,43,67,163\}:$

$$\mathscr{M}_d(p,q) := \exists \ell > 12 \left[q = \widetilde{\boldsymbol{y}}_{2^{2\ell+1}}(d)/h_d \;\&\; p \mid q \;\&\; p \geqslant 2^{2\ell+2} \right].$$

where $\langle \widetilde{\boldsymbol{y}}_i(d) \rangle_{i \in \mathbb{N}}$ is the strictly ascending sequence[11] consisting of all non-negative integer solutions to the said equation $d\,y^2 + 1 = \square$ and the values of h_d are as shown in the following table:

d	2	3	7	11	19	43	67	163
h_d	1	1	3	1	39	1	351	3135
					$= 3 \cdot 13$		$= 3^3 \cdot 13$	$= 3 \cdot 5 \cdot 11 \cdot 19$

The rationale behind these values of h_d will be explained in Remark 3; anyway, avoiding the division by h_d in the definition of $\widetilde{\boldsymbol{y}}_d$ would only call for minor retouches in the reasoning that will be carried out in Sec. 8.4 and Sec. 8.5.

Independently of representability, each $\mathscr{M}_d$ turns out to satisfy Julia Robinson's exponential growth criteria (†) recalled in Sec. 1 as well as Matiyasevich's condition (‡) seen in Sec. 7.

8.1. Unique-factorization rings of the integers of $\mathbb{Q}(\sqrt{-d}\,)$

Davis' construction of a potential rule-them-all equation exploits a square-free rational integer $d > 0$ such that in the imaginary quadratic field $\mathbb{Q}(\sqrt{-d}\,)$ the algebraic integers[12] form a unique-factorization integral domain $\mathcal{A}_d$. All such numbers were discovered by Carl Friedrich Gauss; they are

1, 2, 3, 7, 11, 19, 43, 67, 163 (see OEISA003173),

and they are often termed ***Heegner numbers*** after the name of the scholar who gave, in the 1950s, a decisive contribution to the proof that no more numbers with the desired property exist (cf. [16, 35]). Number 1 must be discarded beforehand, because it is a perfect square (hence -1 cannot serve as the discriminant of a Pell's equation); moreover, as it turns out that $d \equiv 3 \mod 4$ holds for all other Heegner numbers except $d = 2$, we have:

$$\mathcal{A}_d = \begin{cases} \mathbb{Z}\left[\sqrt{-d}\,\right] & \text{when } d = 2, \\ \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right] & \text{for } d \in \{3,7,11,19,43,67,163\}. \end{cases}$$

[11] This is tightly akin to the sequence $\langle \boldsymbol{y}_i(a) \rangle_{i \in \mathbb{N}}$ seen earlier, since $\boldsymbol{y}_i(a) = \widetilde{\boldsymbol{y}}_i(a^2 - 1)$.

[12] The algebraic integers mentioned here are the elements of $\mathbb{Q}(\sqrt{-d}\,)$ which are roots of monic polynomials $x^n + c_{n-1}x^{n-1} + \cdots + c_0$ with rational integer coefficients c_i .

The rational prime numbers that cease to be prime in this ring $\mathcal{A}_d$ turn out to be the ones writable in the following ***norm form*** (where $w,t \in \mathbb{Z}$):

$$\begin{array}{ll} w^2 + d\,t^2 & \text{when } d = 2, \\ w^2 + w\,t + \frac{d+1}{4}\,t^2 & \text{for } d \in \{3,7,11,19,43,67,163\}. \end{array}$$

(Remark: In the case when $d = 3$, the numbers of this form coincide with the ones writable in the form $w^2 + 3\,t^2$; when $d = 7$, then 2 is the sole prime number of norm form that cannot be written in the form $w^2 + 7\,t^2$).

For any Heegner number d, we call ***inert*** those numbers p, prime in $\mathbb{Z}$, that remain prime in the enlarged ring $\mathbb{Z}\left[\sqrt{-d}\,\right]$. We must make an exception for $p = 2$ relative to $d = 3$: that p remains in fact irreducible, but no longer prime in $\mathbb{Z}\left[\sqrt{-3}\,\right]$;[13] however, it becomes prime in the ring of integers of $\mathbb{Q}(\sqrt{-3}\,)$, which is larger than $\mathbb{Z}\left[\sqrt{-3}\,\right]$. The number d itself is *not* an inert prime.

When $d \neq 2$, a prime p other than d turns out to be *inert* if and only if

$$-d \quad \not\equiv \quad x^2 \mod p \qquad \text{holds for some } x \in \mathbb{Z} \text{ such that } |x| < p\,.$$

According to the quadratic reciprocity law, this also amounts to the property

$$p \quad \not\equiv \quad y^2 \mod d \qquad \text{for any } y \in \mathbb{Z} \text{ such that } 0 < |y| < d\,,$$

which offers a practical criterion for recognizing inert primes.

On these grounds, one easily preps the tables below, showing, relative to each Heegner number $d \neq 1$, which primes are inert/representable:[14]

d	inert prime p
2	$p \equiv 5,7 \mod 8$
3	$p \equiv 2 \mod 3$
7	$p \equiv 3,5,6 \mod 7$
11	$p \equiv 2,6\,..\,8,10 \mod 11$
19	$p \equiv 2,3,8,10,12\,..\,15,18 \mod 19$
43	$p \equiv 2,3,5,7,8,12,18\,..\,20,22,26\,..\,30,32\,..\,34,37,39,42 \mod 43$
67	$p \equiv 2,3,5,7,8,11\,..\,13,18,20,27,28,30\,..\,32,34,$ $38,41\,..\,46,48,50\,..\,53,57,58,61,63,66 \mod 67$
163	$p \equiv 2,3,5,7,8,11\,..\,13,17\,..\,20,23,27\,..\,32,37,42,44,45,48,50,52,59,63,$ $66\,..\,68,70,72,73,75,76,78\,..\,80,82,86,89,92,94,98,99,101\,..\,103,$ $105\,..\,110,112,114,116,117,120,122\,..\,125,127\,..\,130,$ $137\,..\,139,141,142,147\,..\,149,153,154,157,159,162 \mod 163$

[13] To see that 2 is not prime in $\mathbb{Z}\left[\sqrt{-3}\,\right]$, it suffices to observe that 2 divides $4 = (1 + \sqrt{-3})\,(1 - \sqrt{-3})$ without dividing either factor; on the other hand 2 is irreducible in $\mathbb{Z}\left[\sqrt{-3}\,\right]$, in the sense it can be factorized as $2 = (a + b\sqrt{-3})\,(a' + b'\sqrt{-3})$ only with $b = b' = 0$ and $a = \pm 1 \vee a' = \pm 1$.

[14] Herein, the notation $h\,..\,k$ designates the integer range $\{h, h+1, \ldots, k\}$.

d	representable prime q other than d
2	$q \equiv 1, 3 \mod 8$
3	$q \equiv 1 \mod 3$
7	$q \equiv 1, 2, 4 \mod 7$
11	$q \equiv 1, 3..5, 9 \mod 11$
19	$q \equiv 1, 4..7, 9, 11, 16, 17 \mod 19$
43	$q \equiv 1, 4, 6, 9..11, 13..17, 21, 23..25, 31, 35, 36, 38, 40, 41 \mod 43$
67	$q \equiv 1, 4, 6, 9, 10, 14..17, 19, 21..26, 29, 33, 35..37, 39, 40, 47, 49, 54..56, 59, 60, 62, 64, 65 \mod 67$
163	$q \equiv 1, 4, 6, 9, 10, 14..16, 21, 22, 24..26, 33..36, 38..41, 43, 46, 47, 49, 51, 53..58, 60..62, 64, 65, 69, 71, 74, 77, 81, 83..85, 87, 88, 90, 91, 93, 95..97, 100, 104, 111, 113, 115, 118, 119, 121, 126, 131..136, 140, 143..146, 150..152, 155, 156, 158, 160, 161 \mod 163$

In [8], inert primes are called *poison primes*, because they 'poison' those $m \in \mathbb{N}$ in whose standard factorization they appear with an odd exponent, in the following sense: if m gets so poisoned, then it is not representable in the above-specified quadratic form. We sum up the situation in the frame shown here:

Inert, or '*poison*' prime:

- it remains prime;
- it is not representable in the norm form;
- it poisons (by rendering it, in turn, not so representable) any $m \in \mathbb{N}$ in whose standard factorization it occurs with an odd exponent.

Example 1. Take $d = 2$. The argument just developed yields that any representable odd m satisfies either one of the congruences $m \equiv d \pm 1 \mod 8$. $\dashv$

8.2. Promising (Diophantine?) exponential-growth relations

In this section we outline Davis' construction of a potential rule-them-all equation, choosing the Heegner number $d = 67$ as our running example.[15] Before going into technicalities related to that number, we offer some background information.

To each Heegner number $d \neq 1$, there corresponds the Pell equation

$$d\,y^2 + 1 = x^2 \,,$$

trivially solved by $y_0 = 0\,,\, x_0 = 1$. Its fundamental solution $y_1\,,\, x_1$ (namely, the one with y, x positive integers of smallest possible size), and the rule for

[15] In [3], the authors adopted $d = 19$ as running example.

getting from two consecutive solutions y_k, x_k and y_{k+1}, x_{k+1} its next solution y_{k+2}, x_{k+2}, are tabulated here:

d	y_1	x_1	y_{k+2}	x_{k+2}
2	2	3	$6y_{k+1}-y_k$	$6x_{k+1}-x_k$
3	1	2	$4y_{k+1}-y_k$	$4x_{k+1}-x_k$
7	3	8	$16y_{k+1}-y_k$	$16x_{k+1}-x_k$
11	3	10	$20y_{k+1}-y_k$	$20x_{k+1}-x_k$
19	39	170	$340y_{k+1}-y_k$	$340x_{k+1}-x_k$
43	531	3482	$6964y_{k+1}-y_k$	$6964x_{k+1}-x_k$
67	5967	48842	$97684y_{k+1}-y_k$	$97684x_{k+1}-x_k$
163	5019135	64080026	$2\cdot x_1\cdot y_{k+1}-y_k$	$2\cdot x_1\cdot x_{k+1}-x_k$

A cornerstone in the construction of candidate rule-them-all equations is the following basic fact concerning Pell equations (cf., e.g., [4, Corollary 3.2]):

Lemma 8.1. *Consider the Pell equation $x^2-\delta\,y^2=1$, with $\delta>0$ a non-square integer; let $\langle x_0,y_0\rangle$, $\langle x_1,y_1\rangle$, $\langle x_2,y_2\rangle,\ldots$ be its solutions in $\mathbb{N}$, with $y_0<y_1<y_2<\cdots$. Then the following identities hold for every $\ell\in\mathbb{N}$:*

$$x_{2\ell} \;=\; x_\ell^2+\delta\,y_\ell^2 \quad\text{and}\quad y_{2\ell} \;=\; 2x_\ell\,y_\ell\,. \qquad \dashv$$

This lemma shows that each $x_{2\ell}$ entering in a representation of 1 in the form $x^2-\delta\,y^2$ is, in turn, represented by the quadratic form $x^2+\delta\,y^2$. One can get Lemma 8.1 from the equality $x_k+y_k\sqrt{\delta}=\big(x_1+y_1\sqrt{\delta}\big)^k$ holding for all $k\in\mathbb{N}$, by taking into account the irrationality of $\sqrt{\delta}$. Consequently, since each entry of the sequence $\langle x_{2\ell+1}+y_{2\ell+1}\sqrt{\delta}\rangle_{\ell\in\mathbb{N}}$ equals $\big(x_{2\ell}+y_{2\ell}\sqrt{\delta}\big)\cdot\big(x_1+y_1\sqrt{\delta}\big)$, we have

$$y_{2\ell+1} \;=\; y_1\,x_\ell^2+2x_1\,x_\ell\,y_\ell+\delta\,y_1\,y_\ell^2\,,$$

and so, when δ is one of the d's that interest us here:

$d=2$	$y_{2\ell+1}=2\,(x_\ell+y_\ell)\,(x_\ell+2y_\ell)$
$d=3$	$y_{2\ell+1}=(x_\ell+y_\ell)\,(x_\ell+3y_\ell)$
$d\in\{7,11\}$	$y_{2\ell+1}=(x_\ell+3y_\ell)\,(3x_\ell+d\,y_\ell)$
$d=19$	$y_{2\ell+1}=(3x_\ell+13y_\ell)\,(13x_\ell+3\cdot 19y_\ell)$
$d=43$	$y_{2\ell+1}=(9x_\ell+59y_\ell)\,(59x_\ell+9\cdot 43y_\ell)$
$d=67$	$y_{2\ell+1}=(27x_\ell+221y_\ell)\,(221x_\ell+27\cdot 67y_\ell)$
$d=163$	$y_{2\ell+1}=(627x_\ell+8005y_\ell)\,(8005x_\ell+627\cdot 163y_\ell)$

It turns out that the binomials appearing in each one of the above equalities evaluate to co-prime numbers v_ℓ, w_ℓ; i.e.: $x_\ell+y_\ell\perp x_\ell+2y_\ell$ when $d=2$, $x_\ell+y_\ell\perp x_\ell+3y_\ell$ when $d=3,\ldots,627x_\ell+8005y_\ell\perp 8005x_\ell+102201y_\ell$ when

$d = 163$. Accordingly, if $y_{2\ell+1}$ is representable in the norm form, so are its factors v_ℓ and w_ℓ; in fact, no inert prime could possibly divide either v_ℓ or w_ℓ to an odd power, else it would divide $y_{2\ell+1}$ to the same odd power.[16]

Example 2. Take $d = 67$. To see that $27\,x_\ell + 221\,y_\ell \perp 221\,x_\ell + 1809\,y_\ell$ holds for every ℓ , begin by observing that $x_\ell \perp y_\ell$: in fact, any positive integer t dividing both of x_ℓ and y_ℓ will divide $x_\ell^2 - d\,y_\ell^2$, which equals 1; therefore such a t must equal 1 . Next, by way of contradiction, suppose that a prime number p exists such that $p \mid 221\,x_\ell + 1809\,y_\ell$ and $p \mid 27\,x_\ell + 221\,y_\ell$. Then $p \mid 2\,y_\ell$ holds, because $2\,y_\ell = 27\,(221\,x_\ell + 1809\,y_\ell) - 221\,(27\,x_\ell + 221\,y_\ell)$; therefore, either $p = 2$ or $p \mid y_\ell$ holds. Inspection of the Pell equation at hand, whose discriminant d is odd, shows us that y_ℓ and x_ℓ have opposite parity; so $27\,x_\ell + 221\,y_\ell$ is odd and $p \neq 2$. Hence $p \mid y_\ell$, and moreover $p \mid [11\,(221\,x_\ell + 1809\,y_\ell) - 90\,(27\,x_\ell + 221\,y_\ell)]$, i.e., $p \mid x_\ell + 9\,y_\ell$; thus $p \mid x_\ell$, contradicting the co-primality between x_ℓ and y_ℓ .[17] ⊣

What follows will adjust to the case $d = 67$ a general technique for associating with a given Heegner number $d \neq 1$ an equation whose solutions correspond to the representations of a certain integer C by a quadratic form $d \cdot a^2 \cdot X^2 - b^2 \cdot Y^2$, where X, Y are in turn representable by the quadratic norm form associated with d as seen in Sec. 8.1. In most cases, either $a = 1$ or $b = 1$ or $a = b = 1$ holds; very often C equals 2. Inspection of the complete table of resulting quartic equations shown at the beginning of Sec. 8 makes it evident that the quaternary quartic equation associated with $d = 67$ is relatively elaborate; thus, our running example should encompass all technical difficulties.

Remark 3. Note that $d = 67$ is one of the four cases when $h_d \neq 1$ in the construction of $\mathscr{M}_d$ (see p. 604). The rationale behind this number h_d (for each Heegner number d) is that dividing each y_i by h_d serves to elide the inert primes that occur with an odd exponent in the standard factorization of y_i . ⊣

8.3. Contriving the quaternary quartic associated with $d = 67$

Two lemmas will aid in the proof of a crucial statement to be seen below.

[16] The consideration made in this paragraph needs some refinement for those d's such that $h_d \neq 1$ (see p. 604 and Remark 3 below): this is apparent in the treatment of $d = 7$ in [8] and of $d = 19$ in [3], and will surface again in the treatment of $d = 67$ inside the proof of Thm. 6 below.

[17] For each odd d, the analogous co-primality result is proved very much like in this example, with only the final step requiring a bit of ingenuity. When $d = 3$, the clue is that $2\,(x_\ell + 3\,y_\ell) - (x_\ell + y_\ell) = x_\ell - 5\,y_\ell$. When $d = 7$ or $d = 11$, the clue is that $(x_\ell + 3\,y_\ell) - 3\,y_\ell = x_\ell$; when $d = 19$, the clue is that $9\,(3x_\ell + 13\,y_\ell) - 2\,(13x_\ell + 57\,y_\ell) = x_\ell + 3\,y_\ell$; when $d = 43$, it is that $2\,(59x_\ell + 387\,y_\ell) - 13\,(9x_\ell + 59\,y_\ell) = x_\ell + 7\,y_\ell$; when $d = 163$, it is that $73\,(8005\,x_\ell + 102201\,y_\ell) - 932\,(627\,x_\ell + 8005\,y_\ell) = x_\ell + 13\,y_\ell$. When $d = 2$, the contradiction $p \mid y_\ell \;\&\; p \mid x_\ell$ follows from supposing that a prime number p exists such that $p \mid x_\ell + y_\ell$ and $p \mid x_\ell + 2\,y_\ell$: in fact, $y_\ell = (x_\ell + 2\,y_\ell) - (x_\ell + y_\ell)$ and $x_\ell = 2\,(x_\ell + y_\ell) - (x_\ell + 2\,y_\ell)$.

Lemma 8.2. *Take $d = 67$. For $m, h = 1, 2, 3\ldots$, it holds that*

$$y_{2^m \cdot h} \;=\; 2^m x_h y_h \cdot \textstyle\prod_{0<i<m} x_{2^i \cdot h}\,.$$

In particular, we have

$$y_{2^m} \;=\; 2^{m+1} \cdot \underbrace{3^3 \cdot 13}_{351} \cdot 17 \cdot 24421 \cdot \textstyle\prod_{0<i<m} x_{2^i}\,.$$

Proof. The claim is proved by induction on m: it readily follows from Lemma 8.1 when $m = 1$; moreover, when $m = k+2$, Lemma 8.1 together with the induction hypothesis yields that

$$\begin{aligned} y_{2^m \cdot h} \;=\; y_{2^{k+2} \cdot h} \;=\; 2x_{2^{k+1} \cdot h}\, y_{2^{k+1} \cdot h} &\;=\; 2^{k+2} x_h y_h \cdot \textstyle\prod_{0<i\leqslant k+1} x_{2^i \cdot h} \\ &\;=\; 2^m x_h y_h \cdot \textstyle\prod_{0<i<m} x_{2^i \cdot h}\,. \end{aligned}$$ ⊣

Note that the recursive rule for calculating the y_k's yields, since $y_1 = 351 \cdot 17$, that $351 \mid y_k$ for every k.

Lemma 8.3. *Take $d = 67$. If $y_n/351$ is representable, where $n = 2^m \cdot h$, h is odd, and $m > 0$, then $y_h/351$ is representable.*

Proof. By way of contradiction, suppose that $n = 2^m \cdot h$, h is odd, $m > 0$, but an inert prime p exists dividing $y_h/351$ to an odd power. Since h is odd, y_h is odd and $p \neq 2$. *We know from Lemma 8.1 that $x_{2^i \cdot h}$ is representable for each $i > 0$*: in fact $x_{2^i \cdot h}$ can be written in the form $u^2 + 67v^2$, hence it can also be written as $(u-v)^2 + (u-v)(2v) + 17(2v)^2$, and hence it has the norm form pertaining to $d = 67$. Therefore p divides $x_{2^i \cdot h}$ to an even power (perhaps 0), for $i = 1, \ldots, m-1$. In addition we have $p \nmid 2^m$; moreover, $p \nmid x_h$, because $x_h \perp y_h$. So we finally use Lemma 8.2 to prove that p divides $y_n/351$ to an odd power, thus getting the sought contradiction. ⊣

Here is the above-announced key statement:

Theorem 6. Take $d = 67$. If $y_n/351$ is representable (in the norm form $w^2 + wt + 17t^2$) for some $n > 0$ <u>not</u> a power of 2, then the constraint system

$$\begin{cases} X^2 - 67 \cdot 351^2 \cdot Y^2 = 1, \\ X + 17 \cdot 13^2 \cdot Y = r^2 + rs + 17s^2, \\ 17 \cdot X + 67 \cdot 3^6 \cdot Y = v^2 + vu + 17u^2, \\ Y > 0 \end{cases}$$

has a solution $\bar{X}, \bar{Y}, \bar{r}, \bar{s}, \bar{v}, \bar{u}$ in $\mathbb{Z}$ such that either $\bar{r} \neq \pm 1$ or $\bar{s} \neq 0$ holds and, moreover, $\quad 351 \cdot (\bar{X} + 17 \cdot 13^2 \cdot \bar{Y}) \cdot (17 \cdot \bar{X} + 67 \cdot 3^6 \cdot \bar{Y}) \mid y_n$.

Proof. Suppose $n = 2^m(2\ell + 1)$, with $\ell > 0$, be such that $y_n/351$ is representable. Put $h = 2\ell + 1$. The preceding two lemmas yield—since plainly x_h is even—that $y_{2^m \cdot h}$, and hence $2^m \cdot h$, must be even, m must be positive, and

$y_{2\ell+1}/351$ representable; therefore, $x_\ell + 17\cdot 13^2\cdot\frac{y_\ell}{351}$ and $17\cdot x_\ell + 67\cdot 3^6\cdot\frac{y_\ell}{351}$ are also representable. By setting $\overline{X} = x_\ell$ and $\overline{Y} = \frac{y_\ell}{351}$, we hence have numbers $\bar{r},\bar{s},\bar{v},\bar{u}$ that satisfy the system appearing in the claim.

It is untenable that $\bar{r} = \pm 1 \;\&\; \bar{s} = 0$, because this would imply $x_\ell + 17\cdot 13^2\cdot\frac{y_\ell}{351} = 1$, contradicting $x_\ell > y_\ell \geqslant 5967 = 351\cdot 17$.

Lemma 8.2 tells us that $y_h \mid y_{2^m\cdot h}$; which, in the present context, reads: $351\,(\overline{X}+17\cdot 13^2\cdot\overline{Y})\,(17\overline{X}+67\cdot 3^6\cdot\overline{Y}) = (27\,x_\ell+221\,y_\ell)\,(221\,x_\ell+27\cdot 67\cdot y_\ell) = y_{2\ell+1} \mid y_n$. ⊣

Corollary 1. Under the hypothesis of Thm. 6, the equation

$$67\cdot 3^6\cdot\left(r^2+r\,s+17\,s^2\right)^2 - 13^2\cdot\left(v^2+v\,u+17\,u^2\right)^2 \;=\; 2 \qquad (\S)$$

has a solution $\bar{r}$, $\bar{s}$, $\bar{v}$, $\bar{u}$ such that either $\bar{r}\neq\pm 1$ or $\bar{s}\neq 0$ holds and, moreover, $351\cdot(\bar{r}^2+\bar{r}\,\bar{s}+17\,\bar{s}^2)\cdot(\bar{v}^2+\bar{v}\,\bar{u}+17\,\bar{u}^2) \mid y_n$.

Proof. Indeed, by solving the system of constraints of Thm. 6 in the manner discussed there, we will have

$$\begin{array}{rl} & 67\cdot 3^6\cdot\left(\bar{r}^2+\bar{r}\bar{s}+17\bar{s}^2\right)^2 - 13^2\cdot\left(\bar{v}^2+\bar{v}\bar{u}+17\bar{u}^2\right)^2 \\ = & 67\cdot 3^6\cdot\left(\overline{X}+17\cdot 13^2\cdot\overline{Y}\right)^2 - 13^2\cdot\left(17\cdot\overline{X}+67\cdot 3^6\cdot\overline{Y}\right)^2 \\ = & 67\cdot 3^6\cdot\left(\overline{X}^2+2\cdot 17\cdot 13^2\cdot\overline{X}\cdot\overline{Y}+17^2\cdot 13^4\cdot\overline{Y}^2\right) \\ & -13^2\cdot\left(17^2\cdot\overline{X}^2+2\cdot 17\cdot 67\cdot 3^6\cdot\overline{X}\cdot\overline{Y}+67^2\cdot 3^{12}\cdot\overline{Y}^2\right) \\ = & 2\cdot\left[\overline{X}^2-67\cdot(351\cdot\overline{Y})^2\right] \\ = & 2\,, \end{array}$$

where the ***non-triviality condition*** $\bar{r}\neq\pm 1 \,\vee\, \bar{s}\neq 0$, along with the divisibility constraint stated in the claim, are satisfied. ⊣

8.4. Is $\{\tilde{y}_{2^{2\ell+1}}(67)/351 \,:\, \ell = 0,1,2,\ldots\}$ a Diophantine set?

We continue to refer to the Heegner number 67. Let $\mathcal{H}$ be the assertion:

The equation (§) *admits, altogether, finitely many solutions in integers.*

Then, by combining Cor. 1 with the *preparatory statement* that $y_{2^m}/351$ is representable if and only if m is odd (a fact easily obtainable from the ending remark in the claim of Lemma 8.2, taking into account that 2 is an inert prime while the prime numbers 17 and $24421 = 364\cdot 67+33$ are not inert[18]), we get:

Lemma 8.4. *$\mathcal{H}$ implies that $\{\,y_{2^{2\ell+1}}/351 : \ell\geqslant 0\,\}$ admits a polynomial Diophantine representation.*

[18] The claim that we have emphasized inside the proof of Lemma 8.3 also plays a role here.

Proof. We know from Cor. 1 that if $y_n/351$ is representable for some $n > 1$ not a power of 2, hence of the form $n = 2^m(2\ell+1)$ with $m \geqslant 0$ and $\ell > 0$, then the equation (§) has a non-trivial integer solution $\bar{r}, \bar{s}, \bar{v}, \bar{u}$ such that $351 \cdot (\bar{r}^2 + \bar{r}\,\bar{s} + 17\,\bar{s}^2) \cdot (\bar{v}^2 + \bar{v}\,\bar{u} + 17\,\bar{u}^2) \mid y_n$.

This, along with the preparatory statement, yields the following *sufficient* conditions for the property

$$y \in \{y_{2^{2\ell+1}}/351 : \ell \geqslant 0\} \tag{1}$$

to hold for y:

(i) $y = y_n/351$, for some $n > 1$;

(ii) y is representable in the form $w^2 \pm wt + 17t^2$ with $w, t \in \mathbb{N}$;

(iii) $(\bar{r}^2 + \bar{r}\,\bar{s} + 17\,\bar{s}^2) \cdot (\bar{v}^2 + \bar{v}\,\bar{u} + 17\,\bar{u}^2) \nmid y$, for any solution $\bar{r}, \bar{s}, \bar{v}, \bar{u}$ to (§) such that $\bar{r} \neq \pm 1 \vee \bar{s} \neq 0$.

Here are existential Diophantine definitions, in $\mathbb{N}$, of the first two of these:

(i) $67\,(351\,y)^2 + 1 = \Box \;\;\&\;\; y > 17$ (since $17 = y_1/351$);

(ii) $\exists w \exists t \left[\left(y - (w^2 + 17t^2) \right)^2 = w^2 t^2 \right]$.

Moreover, if (§) admits only finitely many solutions, then also (iii) admits an existential Diophantine definition. Indeed, let $\langle r_1, s_1, v_1, u_1 \rangle, \ldots, \langle r_\kappa, s_\kappa, v_\kappa, u_\kappa \rangle$ be all of the non-trivial solutions to (§) such that $s_i, u_i \in \mathbb{N}$ and $r_i, v_i \in \mathbb{Z}$ for each i. Then (iii) is easily seen to be statable over $\mathbb{N}$ as

$$\begin{aligned}&(\exists q_1, \ldots, q_\kappa, g_1, \ldots, g_\kappa, z_1, \ldots, z_\kappa)\\ &\qquad \&_{i=1}^{\kappa} \Big[y = \left(r_i^2 + r_i s_i + 17 s_i^2\right) \left(v_i^2 + v_i u_i + 17 u_i^2\right) q_i + g_i + 1 \;\; \& \\ &\qquad\qquad g_i + z_i + 2 = \left(r_i^2 + r_i s_i + 17 s_i^2\right) \left(v_i^2 + v_i u_i + 17 u_i^2\right) \Big].\end{aligned}$$

In order to complete the proof that the property (1) is Diophantine when (§) admits only finitely many solutions, it only remains to be shown that (i)–(iii) also are *necessary* conditions for (1) to hold. This will result in a polynomial Diophantine representation of the property $y \in \{y_{2^{2\ell+1}}/351 : \ell \geqslant 0\}$, **if** *the number of solutions to the equation* (§) *is finite* ! (An issue that we are unable to answer.)

Let, hence, $y = y_{2^{2\ell+1}}/351$ hold for some $\ell \geqslant 0$. Obviously (i) holds and, by the preparatory statement made in front of the present lemma, (ii) holds as well.

Towards a contradiction, suppose that we have

$$351\,\left(\bar{r}^2 + \bar{r}\,\bar{s} + 17\bar{s}^2\right)\left(\bar{v}^2 + \bar{v}\,\bar{u} + 17\,\bar{u}^2\right) \mid y_{2^{2\ell+1}} \tag{2}$$

for some non-trivial solution $\bar{r}, \bar{s}, \bar{v}, \bar{u}$ of (§), thus such that

$$67 \cdot 3^6 \cdot \left(\bar{r}^2 + \bar{r}\,\bar{s} + 17\,\bar{s}^2\right)^2 - 13^2 \left(\bar{v}^2 + \bar{v}\,\bar{u} + 17\,\bar{u}^2\right)^2 = 2\,. \tag{3}$$

Now consider the system

$$\left\{\begin{array}{rcrcl} 3^3 \cdot X & + & 13 \cdot 17 \cdot Y & = & 3^3 \cdot \left(\bar{r}^2 + \bar{r}\,\bar{s} + 17\,\bar{s}^2\right)\,, \\ 13 \cdot 17 \cdot X & + & 3^3 \cdot 67 \cdot Y & = & 13 \cdot \left(\bar{v}^2 + \bar{v}\,\bar{u} + 17\,\bar{u}^2\right)\,, \end{array}\right. \tag{4}$$

whose solution is

$$\left\{\begin{array}{rcl} \bar{X} & = & \frac{1}{2}\left[67 \cdot 3^6 \cdot \left(\bar{r}^2 + \bar{r}\,\bar{s} + 17\,\bar{s}^2\right) - 13^2 \cdot 17 \cdot \left(\bar{v}^2 + \bar{v}\,\bar{u} + 17\,\bar{u}^2\right)\right]\,, \\ \bar{Y} & = & \frac{1}{2}\left[3^3 \cdot 13 \cdot \left(\bar{v}^2 + \bar{v}\,\bar{u} + 17\,\bar{u}^2\right) - 3^3 \cdot 13 \cdot 17 \cdot \left(\bar{r}^2 + \bar{r}\,\bar{s} + 17\,\bar{s}^2\right)\right]\,. \end{array}\right.$$

From (3), $\bar{r}^2 + \bar{r}\,\bar{s} + 17\,\bar{s}^2$ and $\bar{v}^2 + \bar{v}\,\bar{u} + 17\,\bar{u}^2$ have the same parity; therefore, the easily checked fact that each non-trivial integer solution $\bar{r}, \bar{s}, \bar{v}, \bar{u}$ to (3)—alias (§)—satisfies $13^2 \cdot 17^2 \cdot (\bar{r}^2 + \bar{r}\,\bar{s} + 17\,\bar{s}^2) < 13^2 \cdot 17 \cdot (\bar{v}^2 + \bar{v}\,\bar{u} + 17\,\bar{u}^2) < 67 \cdot 3^6 \cdot (\bar{r}^2 + \bar{r}\,\bar{s} + 17\,\bar{s}^2)$ entails that $\bar{X}$ and $\bar{Y}$ are positive integers.

From (4) and (3) we get $67 \cdot 3^6 \cdot \left(\bar{X} + \frac{13 \cdot 17}{3^3}\,\bar{Y}\right)^2 - 13^2 \cdot \left(17\bar{X} + \frac{67 \cdot 3^3}{13}\,\bar{Y}\right)^2 = 2$, which simplifies into $\bar{X}^2 - 67\bar{Y}^2 = 1$. Since $\bar{Y} \neq 0$, the latter equation yields $\bar{X} = x_{\bar{g}}$ and $\bar{Y} = y_{\bar{g}}$, for some $\bar{g} \geqslant 1$. Therefore, from (4) and (2) we get $351 \cdot \left(x_{\bar{g}} + 13 \cdot 17 \cdot \frac{y_{\bar{g}}}{3^3}\right) \cdot \left(17\,x_{\bar{g}} + 67 \cdot 3^3 \cdot \frac{y_{\bar{g}}}{13}\right) \mid y_{2^{2\ell+1}}$, i.e., $\left(27\,x_{\bar{g}} + 221\,y_{\bar{g}}\right)\left(221\,x_{\bar{g}} + 27 \cdot 67\,y_{\bar{g}}\right) \mid y_{2^{2\ell+1}}$, i.e., $y_{2\,\bar{g}+1} \mid y_{2^{2\ell+1}}$; this in turn yields $2\,\bar{g} + 1 \mid 2^{2\ell+1}$, a contradiction. ⊣

Corollary 2. $\mathcal{H}$ implies that the relation $\mathscr{M}_{67}\,(p\,,\,q)$, as defined on p. 604, admits a polynomial Diophantine representation.

Proof sketch. In close analogy with the treatment of the Heegner number 3 as provided in [4], it can be shown that

$$\mathscr{M}_{67}\,(u\,,\,v) \iff \left[\,v \in \{y_{2^{2\ell+1}}/351 : \ell > 12\}\,\right] \;\&\; \exists x\left[(2x+1) \cdot u = v\right]$$

is a polynomial Diophantine representation of $\mathscr{M}_{67}$. A salient remark is that, when $b \neq 0$, the condition $\exists x\left[(2x+1) \cdot a = b\right]$ means "$a \mid b$ and a is divisible by any power of 2 that divides b"; thus, since $2^{2\ell+2}$ is the largest power of 2 dividing $y_{2^{2\ell+1}}$, in the case at hand $\exists x\left[(2x+1) \cdot u = v\right]$ amounts to $u \mid v \;\&\; u \geqslant 2^{2\ell+2}$. ⊣

Also the proof that $\mathscr{M}_{67}$ satisfies the exponential-growth criteria that are recalled in the Introduction parallels the treatment of the Heegner number 3 as provided in [4].

8.5. $\mathscr{M}_d$ conforms to property (‡): proofs for two emblematic cases

As announced in the lines that precede Sec. 8.1, Matiyasevich's property (‡) (see p. 602) is satisfied by each $\mathscr{M}_d$ with $d \in \{2,3,7,11,19,43,67,163\}$. The proofs are akin to one another for all d's, just slightly simpler when $d \in \{2,7\}$. To illustrate how they proceed, let us again choose $d = 67$ as our representative case study. We will take the following two facts for granted, one of which is already entered in the proof that $\mathscr{M}_{67}$ has exponential growth, while the other is proved as [4, Lemma 6.9]:

Fact 1. For $n > 1$, it holds that $48842^{n-1} < y_n$.

Fact 2. For every real number $x \geqslant 1$, some positive *even* integer lies in the open interval $I_x :=]\,1+\log_2(1+x)\,,\,5+2\log_2 x\,[$.

Theorem 7. Take $d = 67$. Let $\alpha = 48842^4$, $\beta = 2$, $\gamma = 2^7$, and $\delta = 48842^3$. Then, to each positive integer w there correspond non-negative integers u, v such that

$$\mathscr{M}_d\,(u\,,\,v) \;\;\&\;\; u < \gamma w^{\beta} \;\;\&\;\; v > \delta\,\alpha^{w}\,.$$

Proof. Recalling that

$$\mathscr{M}_{67}\,(u\,,\,v) \quad := \quad \exists \ell \left[\ell > 12 \;\;\&\;\; v = y_{2^{2\ell+1}}/351 \;\;\&\;\; u \mid v \;\;\&\;\; u \geqslant 2^{2\ell+2} \right],$$

in order to prove the claim it suffices to show that, for each $w \geqslant 1$, there is an integer $\ell > 12$ such that

$$2^{2\ell+2} < \gamma w^{\beta} \;\;\&\;\; y_{2^{2\ell+1}} > \delta\,\alpha^{w}\,.$$

Note that Fact 1 yields $y_{2^{2\ell+1}} \geqslant 48842^{2^{2\ell+1}-1}$, for every $\ell \in \mathbb{N}$. Our task, hence, further reduces to proving that, for each $w \geqslant 1$, there is an $\ell > 12$ such that

$$2^{2\ell+2} < \gamma w^{\beta} \;\;\&\;\; 48842^{2^{2\ell+1}-1} > \delta\,\alpha^{w}\,,$$

namely,

$$2^{2\ell+2} < 2^7\,w^2 \;\;\&\;\; 48842^{2^{2\ell+1}-1} > 48842^3 \cdot 48842^{4w}\,,$$

i.e.,

$$2^{2\ell} < 2^5\,w^2 \;\;\&\;\; 48842^{2^{2\ell+1}} > 48842^4 \cdot 48842^{4w}\,. \tag{5}$$

For $w \geqslant 1$, (5) amounts to

$$2\ell < 5 + 2\,\log_2 w \;\;\&\;\; 2^{2\ell+1} > 4 + 4w\,. \tag{6}$$

In turn, $2^{2\ell+1} > 4+4w$ amounts to

$$2\ell > 1+\log_2(1+w)\,,$$

and hence (6) is equivalent to

$$1+\log_2(1+w) < 2\ell < 5+2\log_2 w\,. \tag{7}$$

Summing up, to get the desired claim it suffices to show that, for every $w \geqslant 1$, there is an $\ell \in \mathbb{N}$ satisfying (7). But this readily follows from Fact 2. ⊣

Remark 4. We have selected $d = 67$ as our primary case study in this section, because this case is comparatively challenging; however, we wish to highlight the modifications needed in the proof of Thm. 7 to establish the analogous statement for the Heegner number $d = 2$. ⊣

Theorem 8. Take $d = 2$. Let $\alpha = 3$, $\beta = 2$, $\gamma = 2^6$, and $\delta = 1$. Then, to each positive integer w there correspond non-negative integers u, v such that

$$\mathscr{M}_d(u, v) \ \ \& \ u < \gamma w^{\beta} \ \ \& \ v > \delta\,\alpha^{w}\,.$$

Proof sketch. Now we must refer to the definition:

$$\mathscr{M}_2(u, v) \ \ := \ \ \exists \ell \Big[\ell > 4 \ \& \ v = y_{2^\ell} \ \& \ u \mid v \ \& \ u \geqslant 2^{\ell+1} \Big].$$

Our previous formulations of Fact 1 can be superseded by the following:

- For every positive integer n, it holds that $3^{n-1} < y_n$ (whence $y_{2^\ell} \geqslant 3^{2^\ell - 1}$).

Our goal becomes the one of proving, for each $w \geqslant 1$, the existence of an $\ell > 4$ such that either the condition

$$2^{\ell+1} < \gamma w^{\beta} \ \ \& \ \ y_{2^\ell} > \delta\,\alpha^{w}\,,$$

or the stronger condition

$$2^{\ell+1} < \gamma w^{\beta} \ \ \& \ \ 3^{2^\ell - 1} > \delta\,\alpha^{w}\,,$$

holds. The latter condition, namely $2^{\ell+1} < 2^6 w^2 \ \ \& \ \ 3^{2^\ell-1} > 3^w$, gets rewritten as $2^\ell < 2^5 w^2 \ \ \& \ \ 3^{2^\ell} > 3^{w+1}$, then as $\ell < 5+2\log_2 w \ \ \& \ \ 2^\ell > 1+w$, and then as $\log_2(1+w) < \ell < 5+2\log_2 w$. Fact 2 ensures the existence of such an ℓ. ⊣

8.6. Discovering solutions to $2\cdot\left(r^2+2s^2\right)^2 - \left(u^2+2v^2\right)^2 = 1$

The surmise that each r.e. set admits a singlefold polynomial Diophantine representation was made by Yuri Matiyasevich in 1974, inside the paper where he first proved the singlefold *exponential* Diophantine representability of any r.e. set (cf. [25, p. 301]). It appears promising—yet tantalizing—that the truth of the weaker conjecture that each r.e. set admits a finitefold polynomial Diophantine representation could be established by just proving that a single fourth-degree Diophantine equation has only a finite number of integer solutions. No algorithm can tell us, for any given Diophantine equation, whether the set of its integer solutions is finite or infinite (cf. [9]);[19] nevertheless, the structure of our eight candidate rule-them-all equations is so simple that we may hope that the finitefold-ness of at least one of them will come to light.[20]

For quite a while the authors hoped that Matiyasevich's surmise could be established by just proving that $\langle \bar{r}, \bar{s}, \bar{u}, \bar{v} \rangle = \langle 1, 0, 1, 0 \rangle$ is the sole solution, in $\mathbb{N}$, to the quaternary quartic $2 \cdot \left(r^2 + 2\,s^2\right)^2 - \left(u^2 + 2\,v^2\right)^2 = 1$ corresponding to the Heegner number $d = 2$. In order to detect a non-trivial solution (if any) to this equation, let us associate the equation

$$2A^2 - B^2 = 1 \tag{8}$$

in the unknowns A and B with it. The solutions to this Pell-like equation in $\mathbb{N}$ form the sequence $\langle A_0, B_0 \rangle, \langle A_1, B_1 \rangle, \langle A_2, B_2 \rangle, \ldots$, where

$$A_0 = B_0 = 1 \quad \text{and} \quad A_{n+1} = 3A_n + 2B_n\,, \quad B_{n+1} = 4A_n + 3B_n\,, \tag{9}$$

for all $n \in \mathbb{N}$. Our goal here is to find an integer $n > 0$ such that both of A_n and B_n are representable in the form $w^2 + 2t^2$. We will try to achieve this by means of the method devised by Shanks and Wagstaff [34].

The recurrence formula (9) gives us: $A_1 = 5$, $B_1 = 7$, $A_2 = 29$, $B_2 = 41$, $A_3 = 169$, $B_3 = 239$, etc. We are less interested in the explicit values of A_n, B_n than in their residue classes modulo 8; hence we form the table

n	1	2	3	4	5	6	7	8	$\ldots$
A_n	5	5	1	1	5	5	1	1	$\ldots$
B_n	7	1	7	1	7	1	7	1	$\ldots$,

[19] Given an arbitrary instance $P = 0$ of Hilbert's 10th problem and a variable x_0 not occurring in P, the equation $x_0 \cdot P = 0$ will have infinitely many integer solutions if and only if the equation $P = 0$ has at least one integer solution. Being able to determine, for any given Diophantine equation $Q = 0$, whether or not it is finitefold, would hence enable one to solve Hilbert's 10th problem. This would contradict the today known undecidability of the latter problem (cf. [10, 11]).

[20] Non-trivial solutions (finitely many, so far) to the quaternary quartics associated with the Heegner numbers 3, 7, and 11 were discovered years ago, as reported in [4, p. 530 and p. 538]. Non-trivial solutions corresponding to the Heegner number 43 were also detected, one of them (jointly found by L. Cuzziol and P. Campochiaro) being

$$\begin{array}{rclrcl} r & = & 2644220400, & s & = & -305590179873, \\ v & = & 2488975045142, & u & = & 134875386175\,. \end{array}$$

namely:

$$\begin{array}{llll}
A_n \equiv 5 \mod 8 & \text{if} & n \equiv 1,2 \mod 4\,, \\
A_n \equiv 1 \mod 8 & \text{if} & n \equiv 3,0 \mod 4\,, \\
B_n \equiv 7 \mod 8 & \text{if} & n \text{ is odd}\,, \\
B_n \equiv 1 \mod 8 & \text{if} & n \text{ is even}\,.
\end{array}$$

In view of the information about representability in $\mathbb{Z}\left[\sqrt{-2}\right]$, as provided in Sec. 8.1 (see, in particular, Example 1), we only need to survey those pairs A_n, B_n whose subscript n is a multiple of 4. In particular:[21]

$5 \,\|\, A_4 = 985 = 5 \cdot 197$, where 5 is inert, and so A_4 is not representable;

$103 \,\|\, B_8 = 103 \cdot 15607$, where 103 is inert, and so B_8 is not representable;

$29 \,\|\, A_{12} = 29 \cdot 1549 \cdot 29201$, where $29 \equiv 5 \mod 8$, hence A_{12} is not representable;

$5 \,\|\, A_{16} = 5 \cdot 5741 \cdot 52734529$, and hence A_{16} is not representable;

$302633 \,\|\, B_{20} = 2297 \cdot 302663 \cdot 3553471$, where $302633 \equiv 7 \mod 8$, hence B_{20} is not representable; and so on.

This empirical approach to finding a pair $\langle A_n, B_n \rangle$ of numbers, both representable, that solves (8) fails for each $n \in \{4, 8, 12, 16, \dots, 100\}$; yet it cannot be excluded that a larger n—even, maybe, infinitely many n's—would work.

As a matter of fact, readily after [3] was published on arXiv, two scholars sent us kind communications that they had found useful solutions to (8). On March 9, 2023, Evan O'Dorney (University of Notre Dame) sent us a Sage program by means of which he had located two non-trivial solutions corresponding to the Pell pairs $\langle A_{128}, B_{128} \rangle$ and $\langle A_{140}, B_{140} \rangle$. Independently of him, the next day Bogdan Grechuk (University of Leicester) sent us explicit values of three non-trivial solutions to $2 \cdot \left(r^2 + 2\,s^2\right)^2 - \left(u^2 + 2\,v^2\right)^2 \;=\; 1$, the first of which is:

$$\begin{array}{rcl}
r_1 & = & 877858705853420680629262000814366081842686551 4367, \\
s_1 & = & 1797139324882565197548134105090153037130149943440, \\
u_1 & = & 5221618295817678692343699483662704959631052331713, \\
v_1 & = & 6739958317343073985310999451965479560858521871624;
\end{array}$$

the components of the third solution—associated with the companion Pell numbers A_{486}, B_{486}—are numbers of roughly 180 decimal digits each (see [3, p. 10]).

It must be mentioned that Apoloniusz Tyszka radically disbelieves Matiyasevich's finitefold representability conjecture[22] that has been, throughout, (and firmly remains) our polar star.

[21] By $p^k \| m$, where p is a prime number and $k, m \in \mathbb{N}$, one states that $p^k \mid m \;\&\; p^{k+1} \nmid m$.

[22] See, among many, `https://arxiv.org/abs/0901.2093`. In [37], A. Tyszka advances a

9. Concluding remarks

One of the questions Yu. Matiyasevich raised, at the outset of his seminal paper [24] on the Diophantine singlefold representability issue, was:

> Suppose a proof is available that each
>
> $$D_a(x_1,\dots,x_\kappa) \;=\; 0, \qquad a\in\mathbb{N},$$
>
> in some indexed family of equations has at most one solution in $\mathbb{N}$. Can we extract from it an effective bound $\mathscr{C}_a$ ensuring, when $x_1=\boldsymbol{\nu}_1 \;,\dots,\; x_\kappa=\boldsymbol{\nu}_\kappa$ is such solution, that $\boldsymbol{\nu}_1,\dots,\boldsymbol{\nu}_\kappa\leqslant\mathscr{C}_a$?

As we recalled and explained in the conclusions of [1], his answer was negative in general, assuming the signature underlying the D_a's comprises exponentiation. Matiyasevich calls "noneffectivizable estimates" [25, 27] this and more general limiting results that follow from the univocal representability, in terms of exponentiation, of any r.e. set. Analogous limiting results about polynomial Diophantine equations would follow if it turned out that any r.e. set admits a finitefold representation in merely polynomial terms. Can such a representation be found? The entire paper has revolved around this question, to whose hoped-for positive answer the material outlined in Sec. 8 might prove useful.

Matiyasevich also discussed in [20] (see [1, pp. 151–152] for a quick account) intriguing consequences that establishing the finitefold Diophantine representability of any r.e. set would entail about the Diophantine characterization of the probability of selecting by chance a program that terminates on every input.

This paper, which merges and extends [2, 3], is a companion to [1]. Two differences with respect to [1] are: • In accordance with the historical path [13, 24], great emphasis is placed on the kinship between exponentiation and bounded universal quantification. • Novel candidate rule-them-all equations have come into play.

Acknowledgements

The authors are indebted with Pietro Corvaja for enlightening conversations about the matters of this paper. Discussions with Pietro Campochiaro (Scuola Superiore di Catania) were also helpful.

conjecture that, if true, would falsify Matiyasevich's finitefold representability conjecture. As pointed out in [36, p. 711], even [11, p. 360] suggests a possibility that "would eliminate the possibility of singlefold definitions for all Diophantine sets".

REFERENCES

[1] D. Cantone, A. Casagrande, F. Fabris, and E. G. Omodeo. The quest for Diophantine finite-fold-ness. *Le Matematiche*, 76(1):133–160, 2021. `https://lematematiche.dmi.unict.it/index.php/lematematiche/article/view/2044`.

[2] D. Cantone, L. Cuzziol, and E. G. Omodeo. A Brief History of Singlefold Diophantine Definitions, Proc. of the 38th Italian Conference on Computational Logic, Udine, Italy, June 21–23, 2023, Agostino Dovier and Andrea Formisano eds., CEUR Workshop Proceedings, vol. 3428, 2023, `https://ceur-ws.org/Vol-3428/paper5.pdf`.

[3] D. Cantone, L. Cuzziol, and E. G. Omodeo. Six equations in search of a finite-fold-ness proof, 2023. `https://arxiv.org/abs/2303.02208`.

[4] D. Cantone and E. G. Omodeo. "One equation to rule them all", revisited. *Rendiconti dell'Istituto di Matematica dell'Università di Trieste (RIMUT)*, 53:525–556, 2021. `https://rendiconti.dmi.units.it/volumi/53/028.pdf`.

[5] M. Davis. *On the theory of recursive unsolvability*. PhD thesis, Princeton University, 1950.

[6] M. Davis. *Computability and Unsolvability*. McGraw-Hill, New York, 1958. Reprinted with an additional appendix, Dover 1983.

[7] M. Davis. Extensions and corollaries of recent work on Hilbert's tenth problem. *Illinois Journal of Mathematics*, 7(2):246–250, 1963.

[8] M. Davis. One equation to rule them all. *Transactions of the New York Academy of Sciences. Series II*, 30(6):766–773, 1968.

[9] M. Davis. On the number of solutions of Diophantine equations. *Proc. Amer. Math. Soc.*, 35(2):552–554, 1972.

[10] M. Davis. Hilbert's tenth problem is unsolvable. *Amer. Math. Monthly*, 80(3):233–269, 1973. Reprinted with corrections in the Dover edition of *Computability and Unsolvability* [6, pp. 199–235].

[11] M. Davis, Yu. Matijasevič, and J. Robinson. Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution. In *Mathematical Developments Arising From Hilbert Problems*, vol. 28 of *Proc. of Symposia in Pure Math.*, pages 323–378, Providence, RI, 1976. Amer. Math. Soc. Reprinted in [32, p. 269ff.].

[12] M. Davis and H. Putnam. A computational proof procedure; Axioms for number theory; Research on Hilbert's Tenth Problem. Technical Report AFOSR TR59-124, U.S. Air Force, October 1959. (Part III reprinted in [29, pp. 411-430]).

[13] M. Davis, H. Putnam, and J. Robinson. The decision problem for exponential Diophantine equations. *Ann. of Math., Second Series*, 74(3):425–436, 1961.

[14] M. D. Davis, R. Sigal, and E. J. Weyuker. *Computability, complexity, and languages - Fundamentals of theoretical computer science*. Computer Science ad scientific computing. Academic Press, 1994.

[15] M. Hausner. Applications of a simple counting technique. *The American Mathematical Monthly*, 90(2):127–129, 1983.

[16] K. Heegner. Diophantische Analysis und Modulfunktionen. *Mathematische Zeitschrift*, 56(3):227–253, 1952.

[17] M. Lisi. Some remarks on the Cantor pairing function. *Le Matematiche*, 62(1):55–65, 2007. `https://lematematiche.dmi.unict.it/index.php/lematematiche/article/view/14`.

[18] J. P. Jones. Diophantine representation of the Fibonacci numbers. *The Fibonacci Quarterly*, 13(1):84–88, 1975.

[19] Ju. V. Matijasevič. Enumerable sets are Diophantine. *Soviet Mathematics. Doklady*, 11(3):354–358, 1970. (Translated from [23]).

[20] Yu. Matiyasevich. Diophantine flavor of Kolmogorov complexity. In *Collected reports of participants of JAF-23 (Yerevan, June 2–5, 2004)*, Transactions of the Institute for Informatics and Automation problems of NAS RA, pages 111–122, Yerevan, 2006.

[21] Yu. Matiyasevich. Existential arithmetization of Diophantine equations. *Annals of Pure and Applied Logic*, 253(2-3):225–233, 2009.

[22] Yu. Matiyasevich. Towards finite-fold Diophantine representations. *Journal of Mathematical Sciences*, 171(6):745–752, Dec 2010.

[23] Yu. V. Matiyasevich. Diofantovost' perechislimykh mnozhestv. *Doklady Akademii Nauk SSSR*, 191(2):279–282, 1970. (Russian. Available in English translation as [19]; translation reprinted in [33, pp. 269–273]).

[24] Yu. V. Matiyasevich. Sushchestvovanie neèffektiviziruemykh otsenok v teorii èkponentsial'no diofantovykh uravneniĭ. *Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR (LOMI)*, 40:77–93, 1974. (Russian. Translated into English as [25]).

[25] Yu. V. Matiyasevich. Existence of noneffectivizable estimates in the theory of exponential diophantine equations. *Journal of Soviet Mathematics*, 8(3):299–311, 1977. (Translated from [24]).

[26] Yu. V. Matiyasevich. *Desyataya Problema Gilberta*. Fizmatlit, Moscow, 1993. English translation: *Hilbert's Tenth problem*. The MIT Press, Cambridge (MA) and London, 1993. French translation: *Le dixième Problème de Hilbert: son indécidabilité*, Masson, Paris Milan Barcelone, 1995. URL: http://logic.pdmi.ras.ru/∼yumat/H10Pbook/.

[27] Yu. V. Matiyasevich. Martin Davis and Hilbert's tenth problem. In Omodeo and Policriti [29], pages 35–54.

[28] M. R. Murty and B. Fodden. *Hilbert's tenth problem. An Introduction to Logic, Number Theory, and Computability*, volume 88 of *Student mathematical library*. American Mathematical Society, Providence, RI, 2019.

[29] E. G. Omodeo and A. Policriti, editors. *Martin Davis on Computability, Computational Logic, and Mathematical Foundations*, volume 10 of *Outstanding Contributions to Logic*. Springer, 2016.

[30] J. Robinson. Existential definability in arithmetic. *Transactions of the American Mathematical Society*, 72(3):437–449, 1952. Reprinted in [32, p. 47ff.].

[31] J. Robinson. Diophantine decision problems. In W. J. LeVeque, editor, *Studies in Number Theory*, volume 6 of *Studies in Mathematics*, pages 76–116. Mathematical Association of America, 1969.

[32] J. Robinson. *The collected works of Julia Robinson*, volume 6 of *Collected Works*. American Mathematical Society, Providence, RI, 1996. ISBN 0-8218-0575-4. With an introduction by Constance Reid. Edited and with a foreword by Solomon Feferman. xliv+338 pp.

[33] G. E. Sacks, editor. *Mathematical Logic in the 20th Century*. Singapore University Press, Singapore; World Scientific Publishing Co., Inc., River Edge, NJ, 2003.

[34] D. Shanks and S. S. Wagstaff, Jr. 48 more solutions of Martin Davis's quaternary quartic equation. *Mathematics of Computation*, 64(212):1717–1731, 1995.

[35] H. M. Stark. On the gap in the theorem of Heegner. *Journal of Number Theory*, 1(1):16–27, 1969.

[36] A. Tyszka. A hypothetical way to compute an upper bound for the heights of solutions of a Diophantine equation with a finite number of solutions. In M. Ganzha, L. A. Maciaszek, and M. Paprzycki, editors, *2015 Federated Conference on Computer Science and Information Systems, FedCSIS 2015, Lódz, Poland, September 13-16, 2015*, volume 5 of *Annals of Computer Science and Information Systems*, pages 709–716. IEEE, 2015.

[37] A. Tyszka. A hypothetical upper bound on the heights of the solutions of a Diophantine equation with a finite number of solutions. *Open Comput. Sci.*, 8(1):109–114, 2018.

D. CANTONE
Dept. of Mathematics and Computer Science
University of Catania, Italy
e-mail: `domenico.cantone@unict.it`

L. CUZZIOL
e-mail: `lucacuzz95@gmail.com`

E. G. OMODEO
Dept. of Mathematics, Informatics, and Geosciences
University of Trieste, Italy
e-mail: `eomodeo@units.it`