Rend. Istit. Mat. Univ. Trieste
Vol. 53 (2021), Art. No. 28, pp. 1–32 (electronic)
DOI: 10.13137/2464-8728/33314

# "One equation to rule them all", revisited

Domenico Cantone and Eugenio G. Omodeo

*"Dedicated with friendship to Eugenio for his 70-th birthday by his coauthor"*

Abstract. *If the quaternary quartic equation*

$$9 \cdot \left(u^2 + 7\,v^2\right)^2 - 7 \cdot \left(r^2 + 7\,s^2\right)^2 \quad = \quad 2 \qquad (*)$$

*which M. Davis put forward in 1968 has only finitely many solutions in integers, then — it was observed by M. Davis, Yu. V. Matiyasevich, and J. Robinson in 1976 — every listable set would turn out to admit a single-fold Diophantine representation.*
*In 1995, D. Shanks and S. S. Wagstaff conjectured that* (*) *has* in*finitely many solutions; while in doubt, it seemed wise to us to single out new candidates for the role of "rule-them-all equation". We offer three new quaternary quartic equations, each obtained by much the same recipe which led to* (*)*. The significance of those can be supported by arguments analogous to the ones found in Davis's original paper; moreover, they might play a key role in settling the conjecture that every listable set has a single-fold (or, at least, a finite-fold) representation.*
*Directly from the unproven assertion that any of the novel equations has only finitely many solutions in integers, one can construct a Diophantine relation of exponential growth, as we show in detail for one, namely*

$$3 \cdot \left(r^2 + 3\,s^2\right)^2 - \left(u^2 + 3\,v^2\right)^2 \quad = \quad 2\,,$$

*of the new candidate rule-them-all equations.*
*An account of Julia Robinson's earliest Diophantine reduction of exponentiation to any relation of exponential growth is also included, for the sake of self-containedness.*

Keywords: Hilbert's 10th problem, exponential-growth relation, single/finite-fold Diophantine representation, Pell's equation.
MS Classification 2020: 03D25, 11D25.

## Introduction

In his paper [3], Martin Davis derived from the unproven assertion

> *the equation*
> $$9 \cdot \left(u^2 + 7\,v^2\right)^2 - 7 \cdot \left(r^2 + 7\,s^2\right)^2 \quad = \quad 2 \qquad (*)$$
> *has no solution in non-negative integers save the trivial* $u = r = 1$, $v = s = 0$

that

> *there is no uniform algorithm for testing polynomial Diophantine equations for solvability in positive integers, i.e., Hilbert's tenth problem is unsolvable.*

Yuri Matiyasevich did establish, short afterwards [13], the algorithmic unsolvability of Hilbert's $10^{\text{th}}$ problem, but along a different pattern. Also, Davis's expectation that his quaternary quartic had no non-trivial solutions came to an end in the early 1970s, when new solutions where discovered (see [7] and [22, p. 68]).

Davis's equation still retains, notwithstanding, part of its original fascination (cf. [15, pp. 43–44]). For, on the one hand, it would suffice that (*) had only *finitely many* solutions in integers in order that it can be exploited in the manner originally proposed by Davis — namely, to show that some Diophantine relation has exponential growth. On the other hand, if the number of solutions to (*) is finite, then — according to [4] — it can be shown that a *single-fold* Diophantine representation of the dyadic relation $2^n = c$ can be constructed. More generally, every partial recursive function $\mathcal{F}$ — mapping a subset of $\mathbb{N}^m$ into $\mathbb{N} = \{0, 1, \dots\}$, for some $m$ — could be represented as

$$\mathcal{F}(\boldsymbol{a}_1, \dots, \boldsymbol{a}_m) = \boldsymbol{b} \iff \begin{array}{l}\text{the equation } P\,(\boldsymbol{a}_1, \dots, \boldsymbol{a}_m, x_0, \dots, x_k) = \boldsymbol{b} \\ \text{has a solution in non-negative integers,}\end{array}$$

where $P(a_1, \dots, a_m, x_0, \dots, x_\kappa)$ is a polynomial with integer coefficients in the variables $a_1, \dots, a_m, x_0, \dots, x_\kappa$ such that the following implication holds all over $\mathbb{N}$:[1]

$$(\forall\, a_1, \dots, a_m, b, x_0, \dots, x_\kappa, y_0, \dots, y_\kappa)\Big[ P(a_1, \dots, a_m, x_0, \dots, x_\kappa) = b = P(a_1, \dots, a_m, y_0, \dots, y_\kappa) \Longrightarrow \bigwedge_{i=0}^{\kappa} (x_i = y_i)\Big].$$

[1] It should be clear that the variables $a_1, \dots, a_m$, $b$ and $x_0, \dots, x_\kappa$ play different roles: $b$ and the $a_i$'s act as parameters, whereas the $x_j$'s act as unknowns.

It is conjectured in [23, p. 1720] that (*) has *in*finitely many solutions in integers; while in doubt, it hence seemed wise to us to single out additional candidates for the role of "rule-them-all equation", in the hope that one would prove easier to analyze than the others. One of three alternatives which we put forward in this paper is the novel quaternary quartic equation

$$3 \cdot \left(r^2 + 3\,s^2\right)^2 - \left(u^2 + 3\,v^2\right)^2 \quad = \quad 2\,, \qquad (\overset{*}{*})$$

which emerged from private discussions with Martin Davis.

We shall argue on the significance of this equation by paralleling the arguments found in [3] very closely — even verbatim at various places. Directly from the unproven assertion, $\mathcal{H}$, that $(\overset{*}{*})$ has only finitely many solutions in integers, we shall show how to construct a Diophantine relation $\varrho$ of exponential growth. The same task can be carried out, likewise, with either one of two more quaternary quartic equations which will be presented without detailed treatment.

Davis' original equation as well as the ones that will be considered in the ongoing are of the following type: given a positive non-square integer $\delta$, the solutions to the equation correspond to the representations of a certain integer $c$ by a quadratic form $f(x, y)$ of discriminant $\delta$ (up to squares), where $x, y$ are in their turn representable by a quadratic form of discriminant $-d$ (for a number $d$ simply related to $\delta$, often coinciding with it). The key point is Lemma 3.4, which refers to the discriminant $-3$ but can be generalized to an arbitrary discriminant $-\delta$, as by Corollary 3.2.

An ending proposition of this paper, namely Theorem 6.10, shows that our relation $\varrho$ enjoys a property which, after Matiyasevich [12], we expect to play a crucial role in the hoped-for *finite-fold* representability of all partial recursive functions, which $\mathcal{H}$ would yield if true. (Finite-fold-ness is a weaker requirement than single-fold-ness, as we are about to explain.)

For the sake of self-containedness, in Appendix A we offer a slightly retouched account of Julia Robinson's earliest Diophantine reduction of exponentiation, $b^n = c$, to *any* exponential-growth dyadic relation.

## 1. The finite-fold-ness issue

As was anticipated in [5] and then conclusively shown in 1961 [6], every partial recursive function $\mathcal{F}$ from a subset of $\mathbb{N}^m$ into $\mathbb{N}$ can be specified in the form

$$\mathcal{F}(a_1, \ldots, a_m) = b \quad \Longleftrightarrow \quad (\exists\, x_0 \cdots \exists\, x_\kappa)\ \varphi(\overbrace{\underbrace{a_1, \ldots, a_m, b}_{\text{parameters}}\,,\ \underbrace{x_0, \ldots, x_\kappa}_{\text{unknowns}}}^{\text{pairwise distinct variables}})\,, \qquad (\dagger)$$

for some formula $\varphi$ that only involves:

- individual variables, including (as free variables) the shown ones,
- positive integer constants,
- addition, multiplication, *exponentiation* (namely the predicate $x^y = z$),
- the logical connectives $\mathscr{E}$, $\vee$, $\exists\,\nu$, $=$.

This result, known as the Davis-Putnam-Robinson (or 'DPR') theorem, was later improved by Yu. Matiyasevich in two respects: in [13] he showed how to ban use of exponentiation, altogether, from (†); in [14], while retaining exponentiation, he achieved *single-fold*-ness of the representation, in the sense explained below.[2]

A representation $(\exists\, x_0, \ldots, x_\kappa)\ \varphi$ of $\mathcal{F}$ in the above form (†) is said to be ***single-fold*** if

$$(\forall\, a_1\,, \ldots,\, a_m\,,\, b)\ (\exists\, y_0\,, \ldots,\, y_\kappa)\ (\forall\, x_0\,, \ldots,\, x_\kappa)\Big[\ \varphi \implies \bigwedge_{i=0}^{\kappa} \big(\, x_i \ \ = \ \ y_i \,\big)\ \Big]$$

(i.e., the constraint $\varphi(\, a_1, \ldots, a_m, b\,,\, x_0, \ldots, x_\kappa\,)$ never has multiple solutions). The definition of ***finite-fold***-ness is akin: the overall number of solutions (in the $x$'s) that correspond to each $(m+1)$-tuple $\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_m, \boldsymbol{b}\rangle$ of actual parameters must be finite; or, to state this formally:

$$(\forall\, a_1\,, \ldots,\, a_m\,,\, b)\ (\exists\, s)\ (\forall\, x_0\,, \ldots,\, x_\kappa)\Big[\ \varphi \implies s \geqslant x_0 + \cdots + x_\kappa\ \Big].$$

In [12], Matiyasevich argues on the significance of combining his two improvements to DPR, and on the difficulty — as yet unsolved — of this reconciliation. Full elimination of exponentiation from (†) is generally achieved in two phases: one first gets the polynomial Diophantine representation of a relation of *exponential growth* (see [18, 19]), and then integrates this representation with additional constraints in order to represent the predicate $x^y = z$ polynomially. Unfortunately, though, the solutions to the equations introduced in the first phase have a periodic behavior, causing the equations that specify exponentiation to have infinitely many solutions.

One way out of this difficulty was indicated in [4], and has been recently recalled in [12, 15]: If one managed to prove that there are only a finite number of solutions to a certain quaternary quartic equation, which M. Davis put

---

[2] A virtue of the representation proposed in [14] is that exponentiation occurs in it only once; the author was in fact able to ensure single-fold-ness while reducing (†) to the elegant format

$\mathcal{F}(a_1, \ldots, a_m) = b \iff (\exists\, x_0\,,\, x_1\,, \ldots, x_\kappa)\ Q(a_1, \ldots, a_m, b,\, x_1\,, \ldots, x_\kappa) \,=\, 4^{x_0} + x_0\,,$
where $Q$ is a polynomial with coefficients in $\mathbb{Z}$, devoid of occurrences of $x_0$.

forward in his "*One equation to rule them all*" [3], then a relation of exponential growth could be represented by a single-fold Diophantine polynomial equation.

Skepticism concerning the finitude of the set of solutions to Davis's equation began to circulate among number theorists after D. Shanks and S. S. Wagstaff [23] discovered some fifty elements of this set. This is why we sought new candidates to the role of 'rule-them-all' equation, by resorting to much the same recipe which enabled Davis to obtain his own.

## 2. Davis' quaternary equation and its siblings

As of today, there are four competitors for the role of *'rule-them-all' 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:** $$7 \cdot \left(r^2 + 7\,s^2\right)^2 - 3^2 \cdot \left(u^2 + 7\,v^2\right)^2 \;=\; -2 \quad \text{(the one of [3])};$$

**−11:** $$11 \cdot \left(r^2 + r\,s\, + 3\,s^2\right)^2 - \left(v^2 + v\,u + 3\,u^2\right)^2 \;=\; 2 \;.$$

Each one of these equations stems from a square-free rational integer $d > 0$ such that the integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ form a unique-factorization domain.[3] The numbers in question — detected by Carl Friedrich Gauss — are known to be 1, 2, 3, 7, 11, 19, 43, 67, 163, and no others. Consider, for each such $d$ save $d = 1$, also the equation $d\,y^2 + 1 = \square$ (meaning: '$d\,y^2 + 1$ is a perfect square'). As is well known, this is a Pell equation endowed with infinitely many solutions in $\mathbb{N}$. The equations we have listed are associated — in a manner which will emerge from the discussion in this paper — with the discriminants $-2, -3, -7, -11$ of the corresponding Pell equations; in principle we could have associated a rule-them-all equation also with each one of $-19, -43, -67, -163$.[4]

**Trivial solutions (in $\mathbb{Z}$):** We shall regard as being trivial, for each one of the rule-them-all equations shown above, the following four solutions:

$$r, u \;\in\; \{-1, 1\}\,, \qquad s \;=\; v \;=\; 0 \;.$$

---

[3] The *ring of integers* of an algebraic number field $K$ is the ring of all elements of $K$ which are roots of monic polynomials $x^n + c_{n-1}\,x^{n-1} + \cdots + c_0$ with rational integer coefficients $c_i$ .

[4] Note added in proof. After the writing of this paper was completed, in Dec 2020 and in March 2021, Luca Cuzziol found two more candidate rule-them-all equations, which are:

**−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:** $$43 \cdot \left(s^2 + s\,r\, + 11\,r^2\right)^2 - \left(v^2 + v\,u + 11\,u^2\right)^2 \;=\; 2 \;.$$

When the discriminant is $-11$, two more solutions must be regarded as trivial:

$$r = \pm 1\,, \qquad u = 1\,, \qquad s = 0\,, \qquad v = -1\ .$$

Presently, for the discriminant $-2$, we only know trivial solutions.

**Non-trivial solutions (in $\mathbb{N}$)**: As mentioned at the end of Sec. 1, over 50 solutions were found for the rule-them-all equation with discriminant $-7$.

Two non-trivial solutions for the discriminant $-3$ and two for the discriminant $-11$ were also detected; they will be shown later (see Fact 3).

Relative to each one of our discriminants $-2, -3, -7, -11$, we have a notion of ***representable number***; to wit, a positive integer which can be written in the corresponding quadratic form (with $u\,, v \in \mathbb{Z}$ ):

**$-2$:** $u^2 + 2\,v^2$ ,

**$-3$:** $u^2 + 3\,v^2$ ,

**$-7$:** $u^2 + u\,v + 2\,v^2$ $\big($note the special case $u^2 + 7\,v^2 = (u-v)^2 + (u-v)\,(2\,v) + 2\,(2\,v)^2$ $\big)$,

**$-11$:** $u^2 + u\,v + 3\,v^2$ $\big($note the special case $u^2 + 11\,v^2 = (u-v)^2 + (u-v)\,(2\,v) + 3\,(2\,v)^2$ $\big)$.

**Clue:** Things are so because the integers of $\mathbb{Q}(\sqrt{-d})$ form the ring:

$$\begin{cases} \mathbb{Z}\left[\,\sqrt{-d}\,\right] & \text{if } d \equiv 1, 2 \ (\bmod\ 4)\,, \\ \mathbb{Z}\left[\,(1+\sqrt{-d})\,/\,2\,\right] & \text{if } d \equiv 3 \ (\bmod\ 4)\,. \end{cases}$$

Rather than discussing at length each of the four candidate rule-them-all equations, in the ongoing we shall only examine how to assemble the one, $\binom{*}{*}$, that corresponds to the discriminant $-3$, and how to construct, directly from the unproven assertion that $\binom{*}{*}$ has only finitely many integer solutions, a finite-fold Diophantine representation of a relation of exponential growth.

## 3. Some properties of solutions to the Pell equation $x^2 - 3\,y^2 = 1$

Let us recall a most basic fact about the Pell equation (cf. [9, pp. 216–217]):

LEMMA 3.1. *The successive non-negative integer solutions to any equation of type* $x^2 - \delta\, y^2 \;=\; 1$, *with* $\delta > 0$ *a non-square integer, are given (for* $n \geqslant 0$*) by*

$$x_n + y_n\sqrt{\delta} \quad = \quad \left(x_1 + y_1\sqrt{\delta}\right)^n \;,$$

*where* $x_1, y_1$ *may be calculated from the fact that* $y_1$ *is the least* $y > 0$ *for which* $1 + \delta\, y^2$ *is a square and* $x_1 = \sqrt{1 + \delta\, y_1^2}$ *.*

It hence follows that $x_{2\ell} + y_{2\ell}\,\sqrt{\delta} = \left(x_\ell + y_\ell\,\sqrt{\delta}\right)^2$ and, consequently:

COROLLARY 3.2. *The solutions to the said equation satisfy the identity*[5]

$$x_{2\ell} + y_{2\ell}\,\sqrt{\delta} = \left(x_\ell^2 + \delta\, y_\ell^2\right) + 2\, x_\ell\, y_\ell\,\sqrt{\delta}\,.$$

Henceforth we shall mainly focus on the treatment of the discriminant $-\delta = -3$, occasionally indicating where differences lie with the numbers $-2$ and $-11$. In the case at hand, we readily have $y_1 = 1$ and $x_1 = 2$.

LEMMA 3.3. $\gcd(x_n, y_n) = 1$.

*Proof.* $t \mid x_n$ and $t \mid y_n$ implies $t \mid (x_n^2 - 3\, y_n^2)$, i.e., $t \mid 1$. □

LEMMA 3.4. *Both of the sequences* $\langle x_n\rangle_{n\in\mathbb{N}}$, $\langle y_n\rangle_{n\in\mathbb{N}}$ *are solutions to the second-order recurrence equation*

$$U_{n+2} \quad = \quad 4\, U_{n+1} - U_n \;\;.$$

(Thus, $\langle x_n\rangle_{n\in\mathbb{N}}$=$\langle 1, 2, 7, 26, 97, 362, \ldots\rangle$ and $\langle y_n\rangle_{n\in\mathbb{N}}$=$\langle 0, 1, 4, 15, 56, 209, \ldots\rangle$.)

*Proof.* Let $\theta = 2 + \sqrt{3}$, $\theta' = 2 - \sqrt{3}$. Then, $\theta + \theta' = 4$, $\theta\theta' = 1$, so that $\theta^2 - 4\,\theta + 1 = 0$. Hence $\theta^{n+2} - 4\,\theta^{n+1} + \theta^n = 0$, for $n \geqslant 0$. That is,

$$x_{n+2} + y_{n+2}\sqrt{3} \;=\; 4\,\left(x_{n+1} + y_{n+1}\sqrt{3}\right) - \left(x_n + y_n\sqrt{3}\right). \qquad \square$$

LEMMA 3.5. *For* $n$ *odd,* $x_n$ *is even and* $y_n$ *is odd. For* $n$ *even,* $x_n$ *is odd and* $y_n$ *is even.*

*Proof.* The result is clear by inspection for $n = 0,\ 1$. It follows, in general, since Lemma 3.4 implies that $x_{n+2} \equiv x_n \pmod 2$, $y_{n+2} \equiv y_n \pmod 2$. □

LEMMA 3.6. *For* $\ell \geqslant 0$*,*

$$x_{2\ell} = x_\ell^2 + 3\, y_\ell^2, \qquad y_{2\ell} = 2\, x_\ell\, y_\ell.$$

---

[5] As stressed in the Introduction, this identity is a cornerstone in the construction of each candidate rule-them-all equation: it shows that $x_{2\ell}$ — entering in a representation of 1 in the form $x^2 - \delta\, y^2$ — is, in its turn, represented by the quadratic form $x^2 + \delta\, y^2$.

*Proof.* Immediate from Corollary 3.2. □

LEMMA 3.7. *Let $h, m > 0$. Then,*

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

*Proof.* For $m = 1$, the result is given by Lemma 3.6. Proceeding by induction (and using Lemma 3.6),

$$y_{2^{m+1} \cdot h} \ = \ 2 \, x_{2^m \cdot h} \, y_{2^m \cdot h} \ = \ 2^{m+1} \, x_h \, y_h \cdot \textstyle\prod_{0<i\leqslant m} x_{2^i \cdot h} \, . \qquad \square$$

COROLLARY 3.8. Let $m > 0$. Then

$$y_{2^m} \quad = \quad 2^{m+1} \cdot \textstyle\prod_{0<i<m} x_{2^i} \ .$$

*Proof.* Take $h = 1$ in Lemma 3.7. □

LEMMA 3.9. *Let $\ell \geqslant 0$. Then*

$$y_{2\,\ell+1} \quad = \quad (x_\ell + 3\, y_\ell)\,(x_\ell + y_\ell) \ .$$

*Proof.* Lemma 3.1 yields

$$\begin{aligned} x_{2\,\ell+1} + y_{2\,\ell+1}\sqrt{3} \quad &= \quad \left(x_\ell + y_\ell\sqrt{3}\right)^2 \, \left(2 + \sqrt{3}\right) \\ &= \quad \left(\left(x_\ell^2 + 3\, y_\ell^2\right) + 2\, x_\ell\, y_\ell\sqrt{3}\right) \, \left(2 + \sqrt{3}\right) . \end{aligned}$$

Hence,

$$y_{2\,\ell+1} = x_\ell^2 + 4\, x_\ell\, y_\ell + 3\, y_\ell^2 = (x_\ell + 3\, y_\ell)\,(x_\ell + y_\ell). \qquad \square$$

LEMMA 3.10. *Let $\ell \geqslant 0$. Then*

$$\gcd(x_\ell + 3\, y_\ell,\ x_\ell + y_\ell) \quad = \quad 1 \ .$$

*Proof.* Suppose that there is a prime number $p$ such that $p \mid x_\ell + y_\ell$ and $p \mid x_\ell + 3\, y_\ell$. Then, since $3\,(x_\ell + y_\ell) - (x_\ell + 3\, y_\ell) = 2\, x_\ell$, either $p = 2$ or $p \mid x_\ell$. But, by Lemma 3.5, $x_\ell$ and $y_\ell$ have opposite parity, so $p \neq 2$. Hence $p \mid x_\ell$, and therefore $p \mid \big((x_\ell + y_\ell) - x_\ell\big)$, i.e., $p \mid y_\ell$, which contradicts Lemma 3.3. □

## 4. Representable numbers

In the case under study, namely when the discriminant has value $-3$, a positive integer $x$ is called ***representable***[6] if there are non-negative integers $u, v$ such that $x = u^2 + 3\, v^2$. If, in addition, $u$ and $v$ are coprime, $x$ will be called

[6] Equivalently (cf. [1]), the positive integers $x$ which interest us here can be characterized as the ones writable in the form $x = s^2 + s\,t + t^2$, with $s, t \in \mathbb{Z}$.

***coprimely representable***. For instance, $3 = 0^2 + 3 \cdot 1^2$ is coprimely representable, as $\gcd(0,1) = 1$, whereas $9 = 3^2 + 3 \cdot 0^2$ is representable but not coprimely representable. Observe that any prime $p$ is representable if and only if it is coprimely representable.

Every perfect square is, trivially, representable. In addition, the product of representable numbers is representable. The latter remark follows readily from the identity

$$\left(u^2 + 3\,v^2\right)\left(r^2 + 3\,s^2\right) = (u\,r - 3\,v\,s)^2 + 3\,(u\,s + v\,r)^2\,. \tag{1}$$

We shall call a prime $p$ ***inert***[7] if $p \equiv 2 \pmod 3$. Note that 3 is the only prime number $q$ such that $q \equiv 0 \pmod 3$; every other prime number either is inert (e.g. $2, 5, 11, 17, 23, 29, \dots$) or satisfies the congruence $q \equiv 1 \pmod 3$ (e.g. $7, 13, 19, 31, 37, \dots$).

LEMMA 4.1. *For an odd prime $p$,*

$$p \text{ is not inert} \quad \Longleftrightarrow \quad \left(\tfrac{-3}{p}\right) \neq -1,$$

*where $\left(\frac{-3}{p}\right)$ is a Legendre symbol.*[8]

*Proof.* For $p = 3$, the lemma holds, since 3 is not inert and $\left(\frac{-3}{3}\right) = 0$. Hence, we may assume that $p > 3$. By the quadratic reciprocity law and the multiplicative property of Legendre symbols, we have

$$(-1)^{\frac{p-1}{2}} = \left(\tfrac{3}{p}\right)\left(\tfrac{p}{3}\right) = \left(\tfrac{-3}{p}\right)\left(\tfrac{-1}{p}\right)\left(\tfrac{p}{3}\right),$$

so that $\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)$. Thus, by applying Euler's criterion to $\left(\frac{-1}{p}\right)$, we have

$$\begin{aligned}\left(\tfrac{-3}{p}\right) &\equiv (-1)^{\frac{p-1}{2}}\left(\tfrac{-1}{p}\right)\left(\tfrac{p}{3}\right) \pmod p \\ &\equiv (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\tfrac{p}{3}\right) \pmod p \\ &\equiv \left(\tfrac{p}{3}\right) \pmod p\,.\end{aligned}$$

---

[7] In [3], Davis dubs 'poison primes' the numbers which play an analogous role relative to the discriminant $-7$. For any discriminant $-d$ that we consider, we regard as 'inert' those primes which remain prime in the enlarged ring $\mathbb{Z}\left[\sqrt{-d}\,\right]$, the only exception being $p = 2$ relative to the discriminant $-3$ (that $p$ remains irreducible, but no longer prime, in $\mathbb{Z}\left[\sqrt{-3}\,\right]$; however, it becomes prime in the ring of integers of $\mathbb{Q}\left(\sqrt{-3}\,\right)$, which is larger than $\mathbb{Z}\left[\sqrt{-3}\,\right]$).

[8] See Appendix B for a definition of Legendre symbols and the statements of some of their main properties.

By applying Euler's criterion to $\left(\frac{p}{3}\right)$ and recalling that $p > 3$, the latter implies that

$$\left(\frac{-3}{p}\right) = 1 \iff \left(\frac{p}{3}\right) = 1 \iff p \equiv 1 \pmod 3 \iff p \text{ is not inert}\,,$$

concluding the proof of the lemma. □

In view of the preceding lemma, since, for an odd prime $p$, $\left(\frac{-3}{p}\right) \neq -1$ if and only if $p \mid z^2 + 3$ for some $z$, we have also the following corollary.

COROLLARY 4.2. For an odd prime $p$,

$$p \text{ is not inert} \quad \iff \quad p \mid z^2 + 3 \text{ for some } z.$$

FACT 1. *An immediate consequence of the preceding corollary is that any non-inert prime divides some coprimely representable number (of the form $z^2 + 3$). In fact, as we shall see later, any non-inert prime is representable (cf. Lemma 4.5).*

We now undertake proving that the representable positive integers are precisely the ones in whose factorization no inert prime number appears with an odd exponent.

We begin with a couple of simple facts:

LEMMA 4.3. *For a coprimely representable integer $x$, the following properties hold:*

(a) *if $2 \mid x$, then $2^2 \mid x$, but $2^3 \nmid x$; in addition, $x/4$ is representable;*[9]

(b) *if $3 \mid x$, then $3^2 \nmid x$.*

*Proof.* Let $x = r^2 + 3\,s^2$, with $r, s$ coprime integers.

(a) Let us assume that $2 \mid x$. Plainly, $2 \nmid r$ and $2 \nmid s$. Thus, we can write $r = 2k + 1$ and $s = 2\ell + 1$, for some integers $k$ and $\ell$. Hence

$$\begin{aligned} x &= (2k+1)^2 + 3\,(2\ell+1)^2 \\ &= 4\,(k^2 + k + 3\ell^2 + 3\ell + 1)\,, \end{aligned}$$

so that $2^2 \mid x$ plainly holds; and since $(k^2 + k + 3\ell^2 + 3\ell + 1)$ is clearly odd, we have also that $2^3 \nmid x$.

Next, to prove that $x/4$ is representable, we shall make use of the following identity:

$$\frac{r^2 + 3s^2}{4} = \left(\frac{r \pm 3s}{4}\right)^2 + 3\left(\frac{r \mp s}{4}\right)^2\,. \tag{2}$$

[9] In fact, it can be shown that $x/4$ is coprimely representable.

Since $r$ and $s$ are odd, then $(r \bmod 4)$, $(s \bmod 4) \in \{1, -1\}$. Thus, either $r+s \equiv 0 \pmod 4$ or $r-s \equiv 0 \pmod 4$. In the former case, we have $r-3s \equiv 0 \pmod 4$, whereas in the latter case $r+3s \equiv 0 \pmod 4$ holds. In other words, either both $\frac{r-3s}{4}$ and $\frac{r+s}{4}$ are integers or so are both $\frac{r+3s}{4}$ and $\frac{r-s}{4}$. In any case, (2) implies that $\frac{x}{4} = \frac{r^2+3s^2}{4}$ is representable.

(b) Let us now assume that $3 \mid x$. Hence, $3 \mid r^2$ so that $3 \mid r$ and $3^2 \mid r$. But then if $3^2 \mid x$, we would have $3^2 \mid 3s$ and therefore $3 \mid s$, contradicting the coprimality of $r$ and $s$. Thus, $3^2 \nmid x$. □

LEMMA 4.4. *If there is an inert prime dividing $x$ to an odd power, then $x$ is not representable.*

*Proof.* Let $p$ be an inert prime dividing $x$ to an odd power, but assume, by way of contradiction, that $x$ is representable, i.e., $x = \bar{u}^2 + 3\,\bar{v}^2$ for some integers $\bar{u}, \bar{v}$. Let $d = \gcd(\bar{u}, \bar{v})$, so that $\bar{u} = d\,u$ and $\bar{v} = d\,v$ for some coprime integers $u, v$. Thus, we have

$$x = d^2\,(u^2 + 3\,v^2)\,, \tag{3}$$

and therefore the prime $p$ must divide $u^2 + 3\,v^2$, i.e.,

$$u^2 + 3\,v^2 \equiv 0 \pmod p\,. \tag{4}$$

We can easily rule out the possibility $p = 2$, since, by (3) and Lemma 4.3, 2 divides $x$ to an even power. Hence $p$ must be an odd prime.

The co-primality of $u, v$ entails that $p \nmid v$, i.e., $v \in \mathbb{Z}_p^*$, so that there exists an integer $z$ such that $v\,z \equiv 1 \pmod p$. Hence, by (3),

$$(u\,z)^2 + 3 \equiv u^2\,z^2 + 3\,v^2\,z^2 \equiv (u^2 + 3\,v^2)\,z^2 \equiv 0 \pmod p$$

and therefore $p \mid (u\,z)^2 + 3$. It follows from Corollary 4.2 that $p$ is not inert, a contradiction. Hence $x$ is not representable. □

LEMMA 4.5. *Every non-inert prime $p$ is representable.*

*Proof.* For $p = 3$ the thesis is obvious. For a non-inert prime $p > 3$, we follow a proof due to Euler, as outlined in [2, p. 11 and pp. 19–20]; its argument, for a prime $q$, consists of two basic steps:

**Reciprocity Step:** if $q \equiv 1 \pmod 3$ (i.e., $q$ is a non-inert prime other than 3), then $q$ divides some coprimely representable integer;

**Descent Step:** if $q > 3$ divides some coprimely representable integer, then $q$ is representable.

Plainly, an application of the Reciprocity Step followed by a Descent Step yields the thesis at once.

The correctness of the Reciprocity Step is an immediate consequence of Corollary 4.2, whereas the correctness of the Descent Step is proved in Appendix C. □

The following lemma inverts Lemma 4.4, thereby yielding a characterization of representable integers as just the non-negative integers which are divided to an odd power by no inert prime.

LEMMA 4.6. *If $x \geqslant 0$ is not representable, then some inert prime divides $x$ to an odd power.*

*Proof.* Let $x$ be a non-representable positive integer. By way of contradiction, let us assume that every inert prime divides $x$ to an even power. Then we have $x = NP^2$, where $N$ is a (possibly empty) product of non-inert primes and $P$ is a (possibly empty) product of inert primes. Plainly, $P^2$ is representable. In addition, $N$ is representable too, since it is the product of non-inert primes and all of them, by Lemma 4.5, are representable. But then $x$ would be representable, as it is the product of the representable numbers $N$ and $P^2$, which is a contradiction. Thus, there must be an inert prime dividing $x$ to an odd power. □

FACT 2. *Let us momentarily shift focus back to the various discriminants introduced in Sec. 2. Each of those has — relative to the associated notion of representability as given in Sec. 2 — a corresponding suitable notion of inertness. In the respective cases,* ***inert primes*** *are:*

| | |
|---|---|
| **$-2$:** | *prime numbers $p$ such that $p \equiv 5, 7 \pmod 8$;* |
| **$-3$:** | *prime numbers $p$ such that $p \equiv 2 \pmod 3$;* |
| **$-7$:** | *prime numbers $p$ such that $p \equiv 3, 5, 6 \pmod 7$;* |
| **$-11$:** | *prime numbers $p$ such that $p \equiv 2, 6, 7, 8, 10 \pmod{11}$.* |

*It can always be proved, as we have discussed only for the discriminant $-3$, that the representable numbers are precisely those positive integers in whose factorization no inert prime appears with an odd exponent. (In particular, a prime number is representable if and only if it is not inert.)*

Next, returning to our main case-study, we prove some representability properties of the $x_i$'s and $y_i$'s defined in Lemma 3.1.

LEMMA 4.7. *For all $m > 0$, $y_{2^m}$ is representable if and only if $m$ is odd.*

*Proof.* Let $m > 0$. By Corollary 3.8, we have

$$y_{2^m} = 2^{m+1} \cdot \prod_{0<i<m} x_{2^i} \,. \tag{5}$$

Let us first assume that $m$ is odd. Then $2^{m+1}$ is representable, since it is a perfect square. In addition, by Lemma 3.6, each factor $x_{2^i}$ in (5) is representable. Thus $y_{2^m}$ is representable, inasmuch as the product of representable numbers.

On the other hand, if $m$ is even, the inert prime 2 divides $y_{2^m}$ to the odd power $m+1$, since all factors $x_{2^i}$ in (5) are odd numbers. Thus, by Lemma 4.4, $y_{2^m}$ is not representable. □

LEMMA 4.8. *Let $n = 2^m \cdot k$, with $k > 0$ an odd number and $m > 0$. If $y_n$ is representable, then so is $y_k$.*

*Proof.* Suppose that $y_n$ is representable, whereas $y_k$ is not. By Lemmas 3.5 and 4.6, there is an odd inert prime $p$ which divides $y_k$ to an odd power. We prove that the inert prime $p$ must also divide $y_n$ to an odd power, thereby yielding a contradiction by Lemma 4.4. From Lemma 3.7, we have

$$y_n \quad = \quad 2^m \, x_k \, y_k \prod_{0<i<m} x_{2^i \cdot k} \;\; . \tag{6}$$

Since by Lemma 3.6 each factor $x_{2^i \cdot k}$ in $y_n$ is representable, Lemma 4.4 implies that $p$ divides each of these numbers to an even (perhaps 0) power. Moreover $p \nmid 2^m$ (since $p$ is odd) and $p \nmid x_k$ (since, by Lemma 3.3, $x_k$ and $y_k$ are coprime). So, by (6), $p$ divides $y_n$ to an odd power, which by Lemma 4.4 contradicts the hypothesis. □

LEMMA 4.9. *Let $\ell \geqslant 0$. If $y_{2\ell+1}$ is representable, so are $x_\ell + 3\,y_\ell$ and $x_\ell + y_\ell$ .*

*Proof.* Let $y_{2\ell+1}$ be representable. From Lemma 3.9, $y_{2\,\ell+1} = (x_\ell + 3y_\ell)(x_\ell + y_\ell)$. In addition, by Lemma 3.10, $x_\ell + 3\,y_\ell$ and $x_\ell + y_\ell$ are coprime. Therefore no inert prime can possibly divide either $x_\ell + 3\,y_\ell$ or $x_\ell + y_\ell$ to an odd power, since otherwise it would divide $y_{2\ell+1}$ to the same odd power. Thus, by Lemma 4.6, both $x_\ell + 3\,y_\ell$ and $x_\ell + y_\ell$ are representable. □

Finally, we obtain:

THEOREM 4.10. *Let $n = 2^m \cdot (2h+1)$, with $m \geqslant 0$ and $h > 0$. If $y_n$ is representable, then the equation*

$$3 \cdot \left(r^2 + 3\,s^2\right)^2 - \left(u^2 + 3\,v^2\right)^2 \quad = \quad 2 \tag{7}$$

*has a non-trivial integer solution $\langle \bar{u}, \bar{v}, \bar{r}, \bar{s} \rangle$ such that $(\bar{u}^2 + 3\,\bar{v}^2)\,(\bar{r}^2 + 3\,\bar{s}^2) \mid y_n$, a solution being dubbed* trivial *when it satisfies $r = \pm 1$ & $s = 0$.*

*Proof.* Let $n = 2^m \cdot (2h+1)$, with $m \geqslant 0$ and $h > 0$, be such that $y_n$ is representable. Then, by Lemma 4.8, $y_{2h+1}$ is representable and therefore, by Lemma 4.9, so are $x_h + 3\,y_h$ and $x_h + y_h$. Thus, there are integers $\bar{u}, \bar{v}, \bar{r}, \bar{s}$ such that

$$\begin{cases} x_h + 3\,y_h &= \bar{u}^2 + 3\,\bar{v}^2 \\ x_h + \;\; y_h &= \bar{r}^2 + 3\,\bar{s}^2\,. \end{cases} \tag{8}$$

Thus,

$$\begin{aligned} & 3\,\left(\bar{r}^2 + 3\,\bar{s}^2\right)^2 - \left(\bar{u}^2 + 3\,\bar{v}^2\right)^2 \\ & = 3\,(x_h + y_h)^2 - (x_h + 3\,y_h)^2 \\ & = 3\,x_h^2 + 6\,x_h\,y_h + 3\,y_h^2 - x_h^2 - 6\,x_h\,y_h - 9\,y_h^2 \\ & = 2\,(\,x_h^2 - 3\,y_h^2\,) = 2\,, \end{aligned}$$

proving that $\langle \bar{u}, \bar{v}, \bar{r}, \bar{s} \rangle$ is an integer solution to (7). In addition, $\langle \bar{u}, \bar{v}, \bar{r}, \bar{s} \rangle$ is non-trivial, else (8) would become

$$\begin{aligned} x_h + 3\,y_h &= 1 \\ x_h + \;\; y_h &= 1\,, \end{aligned}$$

yielding $y_h = 0$, a contradiction, since $h > 0$.

Finally, by (8) and Lemma 3.9,

$$(\bar{u}^2 + 3\,\bar{v}^2)\,(\bar{r}^2 + 3\,\bar{s}^2) = (x_h + 3\,y_h)\,(x_h + y_h) = y_{2h+1}\,,$$

and therefore, by Lemma 3.7, we have

$$(\bar{u}^2 + 3\,\bar{v}^2)\,(\bar{r}^2 + 3\,\bar{s}^2) \mid y_n\,. \qquad \square$$

Fact 3. *The following (relatively) small non-trivial solution to* (7) *was found, and kindly communicated to us on June 26, 2017, by B. Z. Moroz:*

$$r = 16\,, \quad s = 25\,, \quad u = 4\,, \quad v = 35\,.$$

*On August 20, 2017, Dr. Moroz informed us that another non-trivial solution to* (7) *had been detected by Carsten Roschinski.*

*On October 27, 2017, Alessandro Logar communicated to us the following non-trivial solution to* (7)*:*

$$r = 124088\,, \quad s = 7307\,, \quad u = 134788\,, \quad v = 54097\,.$$

*On November 19, 2020, Luca Cuzziol communicated to us two non-trivial solutions to the candidate rule-them-all equation associated with* $-11$ *(see Section 2); they are:*

$$\begin{aligned} & r = 8\,, \quad s = 9\,, \quad v = 30\,, \quad u = 7\,, \quad \textit{and} \\ & r = 8\,, \quad s = 9\,, \quad v = 13\,, \quad u = 17. \end{aligned}$$

Before closing this section, we state and prove some very elementary necessary conditions that any non-trivial solution to (7) must satisfy. To this purpose, we first prove some simple inequalities which hold for every solution to the Pell-type equation

$$3\,x^2 - y^2 = 2$$

related to (7).

LEMMA 4.11. *Let $a, b \geqslant 0$ be integers such that $3\,a^2 - b^2 = 2$. Then $a \leqslant b < 2\,a$. In addition, $a = b$ holds if and only if $a = b = 1$.*

*Proof.* Let $a, b$ be as stated and assume by way of contradiction that $2\,a \leqslant b$, so that $b = 2\,a + k$ holds for some non-negative integer $k$. It follows that $b^2 = (2\,a + k)^2$, whence $3\,a^2 = (2\,a + k)^2 + 2$, yielding the untenable equality $-a^2 = k^2 + 4\,ak + 2$. Hence, $b < 2\,a$ must hold.

Similarly, one can show that the inequality $a \leqslant b$ holds. In addition, if $a = b$, then $2\,a^2 = 2$, yielding immediately $a = b = 1$. □

Then we have

COROLLARY 4.12. Let $\langle \bar{u}, \bar{v}, \bar{r}, \bar{s} \rangle$ be a non-trivial solution to (7) in $\mathbb{N}$. Then

$$\bar{r}^2 + 3\,\bar{s}^2 < \bar{u}^2 + 3\,\bar{v}^2 < 3\left(\bar{r}^2 + 3\,\bar{s}^2\right) .$$

*Proof.* Let $(\bar{u}, \bar{v}, \bar{r}, \bar{s})$ be a non-trivial solution to (7) in $\mathbb{N}$. Since $3\left(\bar{r}^2 + 3\,\bar{s}^2\right)^2 - \left(\bar{u}^2 + 3\,\bar{v}^2\right)^2 = 2$, from Lemma 4.11 we have at once

$$\bar{r}^2 + 3\,\bar{s}^2 \leqslant \bar{u}^2 + 3\,\bar{v}^2 < 3\left(\bar{r}^2 + 3\,\bar{s}^2\right) .$$

In addition, if $\bar{r}^2 + 3\,\bar{s}^2 = \bar{u}^2 + 3\,\bar{v}^2$, then $\bar{r}^2 + 3\,\bar{s}^2 = \bar{u}^2 + 3\,\bar{v}^2 = 1$ and therefore $\bar{r} = \bar{u} = 1$ and $\bar{s} = \bar{v} = 0$, which contradicts the non-triviality of $\langle \bar{u}, \bar{v}, \bar{r}, \bar{s} \rangle$. □

## 5. Is $\{\, y_{2^{2\,\ell+1}} \,:\, \ell = 0, 1, 2, \ldots \}$ a Diophantine set?

Let $\mathcal{H}$ stand for the assertion:

‖ *The equation* (7) *admits, altogether, finitely many solutions in integers.*

Then, by combining Theorem 4.10 with Lemma 4.7, we get:

LEMMA 5.1. *$\mathcal{H}$ implies that $\{\, y_{2^{2\ell+1}} \,:\, \ell \geqslant 0 \,\}$ is a Diophantine set.*

*Proof.* As seen in Lemma 4.7, $y_{2^{2\,\ell+1}}$ is representable for every $\ell \geqslant 0$. In addition, by Theorem 4.10, it follows that if $y_n$ is representable for some $n \geqslant 1$ not a power of 2, hence of the form $n = 2^m\,(2\,h+1)$ with $m \geqslant 0$ and $h > 0$, then the equation (7) has a solution $\langle \bar{u}, \bar{v}, \bar{r}, \bar{s}\rangle$ in $\mathbb{N}$ that differs from $\langle 1,0,1,0\rangle$ and is such that

$$(\bar{u}^2 + 3\,\bar{v}^2)\,(\bar{r}^2 + 3\,\bar{s}^2) \mid y_n\,.$$

The above considerations yield the following *sufficient* conditions in order for the relationship

$$y \in \{y_{2^{2\,\ell+1}} : \ell \geqslant 0\} \tag{9}$$

to hold:

(i) $y = y_n$, for some $n \geqslant 0$;

(ii) $y$ is representable;

(iii) $(u^2 + 3\,v^2)\,(r^2 + 3\,s^2) \nmid y$, for any non-trivial solution $\langle u, v, r, s\rangle$ to (7).

Notice that (i)–(ii) are immediately expressible by existential Diophantine equations:

- $y = y_n$, for some $n \geqslant 0 \quad\Longleftrightarrow\quad (\exists x)(x^2 - 3\,y^2 = 1)$;
- $y$ is representable $\quad\Longleftrightarrow\quad (\exists u,\, v)(y = u^2 + 3\,v^2)$.

Moreover, if (7) admits only finitely many solutions, then also (iii) is expressible by an existential Diophantine equation. Indeed, let $\langle u_0, v_0, r_0, s_0\rangle, \ldots, \langle u_m, v_m, r_m, s_m\rangle$ be the non-trivial solutions to (7). Then (iii) is easily seen to be equivalent to

$$(\exists w_0, \ldots, w_m, z_0, \ldots, z_m, q_0, \ldots, q_m)\Big[\bigwedge_{i=0}^{m} \big(y = (u_i^2 + 3\,v_i^2)\,(r_i^2 + 3\,s_i^2)\,q_i + w_i + 1 \\ \&\; w_i + z_i + 2 = (u_i^2 + 3\,v_i^2)\,(r_i^2 + 3\,s_i^2)\big)\Big]\,.$$

In order to complete the proof that the membership relation (9) is Diophantine when (7) admits only finitely many solutions, it only remains to show that the conditions (i)–(iii) are also necessary for (9) to hold. This will result in a Diophantine specification of the property $y \in \{\, y_{2^{2\ell+1}} \,:\, \ell \geqslant 0\,\}$ **if** *the number of solutions to the novel quaternary quartic,* (7)*, is finite*!

Let, hence, $y = y_{2^{2\,\ell+1}}$ hold for some $\ell \geqslant 0$. Plainly, $y > 0$ and (i) hold and, by Lemma 4.7, (ii) holds as well.

Towards a contradiction, let us assume that we have

$$(\bar{u}^2 + 3\,\bar{v}^2)\,(\bar{r}^2 + 3\,\bar{s}^2) \mid y_{2^{2\,\ell+1}} \tag{10}$$

for some non-trivial solution $(\bar u, \bar v, \bar r, \bar s)$ of (7), thus such that

$$3\,\left(\bar r^2 + 3\,\bar s^2\right)^2 - \left(\bar u^2 + 3\,\bar v^2\right)^2 = 2\,. \tag{11}$$

Let us consider the system

$$\left\{ \begin{array}{rcrcl} X & + & 3\,Y & = & \bar u^2 + 3\,\bar v^2 \\ X & + & Y & = & \bar r^2 + 3\,\bar s^2 \end{array} \right. \tag{12}$$

whose solution is

$$\left\{ \begin{array}{rcl} \overline{X} & = & \frac{1}{2}\left(3\,(\bar r^2 + 3\,\bar s^2) - (\bar u^2 + 3\,\bar v^2)\right) \\ \overline{Y} & = & \frac{1}{2}\left((\bar u^2 + 3\,\bar v^2) - (\bar r^2 + 3\,\bar s^2)\right). \end{array} \right.$$

From (11), $(\bar r^2 + 3\,\bar s^2)$ and $(\bar u^2 + 3\,\bar v^2)$ have the same parity. Thus, by Corollary 4.12, $\overline{X}$ and $\overline{Y}$ are positive integers.

From (12) and (11) we get $3\,(\overline{X}+\overline{Y})^2-(\overline{X}+3\,\overline{Y})^2 = 2$, which simplifies into $\overline{X}^2 - 3\,\overline{Y}^2 = 1$. Since $\overline{Y} \neq 0$, the latter equation yields $\overline{X} = x_{\bar g}$ and $\overline{Y} = y_{\bar g}$, for some $\bar g \geqslant 1$. Hence, by (12) and (10), $\left(x_{\bar g} + 3\,y_{\bar g}\right)\left(x_{\bar g} + y_{\bar g}\right) \mid y_{2^{2\,\ell+1}}$. By Lemma 3.9, the latter implies $y_{2\,\bar g+1} \mid y_{2^{2\,\ell+1}}$, which in its turn yields $2\,\bar g + 1 \mid 2^{2\,\ell+1}$, a contradiction.[10] □

FACT 4. *Let us momentarily shift focus back to the various discriminants $-d$ introduced in Sec. 2. In close analogy with what we have seen in this section and* under assumption *that the corresponding quaternary quartic equation admits at most finitely many solutions in rational integers, one proves that*

$\{\, y_{2^\ell} \,:\, \ell \geqslant 0 \,\}$ is a Diophantine set, when either $d = 2$ or $d = 7$ holds;

$\{\, y_{2^{2\ell+1}} \,:\, \ell \geqslant 0 \,\}$ is a Diophantine set, when either $d = 3$ or $d = 11$ holds

*(where, of course, the sequence $y_n$ of non-negative integer solutions shall be attuned to the corresponding Pell equation $d\,y^2 + 1 = \square$).*

*To the conditions* (i)–(iii)*, one must add the requirement $y > 0$ in the case when no non-trivial solutions are known, namely $d = 2$; for, in that case, condition* (iii) *might hold* vacuously*.*

*Notice that, among the Diophantine conditions which we are considering, the only potential source of multiple solutions is* (ii)*; it may well happen, in fact, that two or more pairs $\langle u, v\rangle \in \mathbb{N}^2$ represent the same positive integer $y$. E.g., with $d = 3$, we have $28 = 1^2 + 3\cdot 3^2 = 4^2 + 3\cdot 2^2 = 5^2 + 3\cdot 1^2$. Anyhow, condition* (ii) *turns out to be* finite-fold*, even in the special case $d = 11$ when it reads*

$$\exists\, v\, \exists\, u\, \left(y = v^2 \pm v\,u + 3\,u^2\right).$$

---

[10] As is well known from the study of Pell equations, $y_h \mid y_\ell \iff h \mid \ell$, for $h, \ell \geqslant 0$.

## 6. A Diophantine set of exponential growth

We begin by deriving some inequalities which show that $y_n$ grows exponentially with $n$.

LEMMA 6.1. $y_{n+1} = x_n + 2\,y_n$ .

*Proof.* Lemma 3.1 yields

$$\begin{array}{rcl} x_{n+1} + y_{n+1}\sqrt{3} & = & \left(x_n + y_n\sqrt{3}\right)\,\left(2+\sqrt{3}\right) \\ & = & (2\,x_n + 3\,y_n) + (x_n + 2\,y_n)\,\sqrt{3}\,, \end{array}$$

which readily gives us the result. □

LEMMA 6.2. *For* $n \geqslant 1$, $\quad 2\,y_n < y_{n+1} \leqslant 4\,y_n$ .

*Proof.* Use Lemmas 6.1 and 3.4. □

LEMMA 6.3. *For* $n \geqslant 1$, $\quad 2^{n-1} \leqslant y_n \leqslant 4^{n-1}$ .

*Proof.* The claim follows by induction from Lemma 6.2. □

In what follows we write

$$\varrho(v,u) \quad :=\quad (\exists\,\ell)\,\left[\,v = y_{2^{2\,\ell+1}}\ \&\ 2^{2\,\ell+2} \mid u\ \&\ u \mid v\,\right]\,.$$

(Notice the implication

$$\varrho(v,u) \quad\Longrightarrow\quad (v \geqslant 4\ \ \&\ \ u \geqslant 4)\,,$$

holding for all $v$ and $u$.)

LEMMA 6.4. *For each* $h \geqslant 0$, *there are* $u, v$ *such that* $\varrho(v,u)$ *and* $v > u^h$.

*Proof.* Given $h \geqslant 0$, choose $N > 0$ such that $r \geqslant N$ implies $2^{r-1} > (2\,r)^h$ . Let $n := 2^{2\,\ell+1}$ be any odd power of 2 such that than $n \geqslant N$ and put $u := 2\,n (= 2^{2\,\ell+2})$ , $v := y_n$. Then, by Corollary 3.8, $\varrho(v,u)$ is true; moreover,

$$\begin{array}{rcll} v & = & y_n & \\ & \geqslant & 2^{n-1} & \text{[by Lemma 6.3]} \\ & > & (2\,n)^h & \\ & = & u^h\,. & \end{array}$$

□

LEMMA 6.5. $\varrho(v,u)$ *implies* $v < u^u$.

*Proof.* $\varrho(v,u)$ implies $u \geqslant 4$ and, therefore, for some $\ell$ such that $u \geqslant 2^{2\ell+2}$ :

$$\begin{array}{rcll} v & = & y_{2^{2\,\ell+1}} & \\ & < & y_u & \\ & \leqslant & 4^{u-1} & \text{[by Lemma 6.3]} \\ & < & u^u\,. & \end{array}$$

□

Finally, we note the relationship:

LEMMA 6.6. $\varrho(v,u) \iff v \in \{y_{2^{2^{\ell+1}}} : \ell \geqslant 0\}$ *&* $OD(u,v)$ *, where* $OD$ *is the following Diophantine relation (to be read "a oddly divides b"):*[11]

$$OD(a,b) \;:=\; (\exists\, x)\; [\,(2\,x+1)\,a = b\,]\,.$$

*Proof.* Clearly $OD(a,b)$ holds — provided $b \neq 0$ — if and only if $a \mid b$ and $a$ is divisible by any power of 2 that divides $b$. E.g.: $OD(a,5)$ holds if and only if $a \in \{1,5\}$; and $OD(a,60)$ holds if and only if $a \in \{4,12,20,60\}$.

Hence it is enough to observe that, by Corollary 3.8 and Lemma 3.5, $2^{2^{\ell+2}}$ is the largest power of 2 that divides $y_{2^{2^{\ell+1}}}$. □

The truth of $\mathcal{H}$ must be left open; however, we have:

THEOREM 6.7. $\mathcal{H}$ *implies that there is a Diophantine relation* $\varrho(v,u)$ *such that*

1. $\varrho(v,u)$ *implies* $v < u^u$ *;*
2. *for each* $\ell \geqslant 0$*, there are* $u$ *and* $v$ *such that* $\varrho(v,u)$ *and* $u^\ell < v$ *.*

*Proof.* We get this at once, with our previously defined $\varrho$, from Lemma 6.6 together with Lemmas 5.1, 6.5, and 6.4. □

As will be further clarified in Appendix A:

COROLLARY 6.8. $\mathcal{H}$ implies that every listable set — namely, the domain of a partial recursive function — is Diophantine, and therefore that Hilbert's tenth problem is algorithmically unsolvable.

*Proof.* For, our Theorem 6.7 yields that $\varrho$'s converse $\mathcal{J}(u,v) := \varrho(v,u)$ meets precisely the well-known conditions of Julia Robinson [18].[12] □

> *The finiteness point is just that if the proof that exponentiation is Diophantine is carried out using my equation or yours, assuming it is known to have finitely many solutions, then the corresponding Diophantine definition of an arbitrary r.e. set will inherit this property: When it has a solution it has only finitely many. This would avoid the situation when the Pell equation is used because it has infinitely many solutions.*
>
> ( Martin Davis, personal letter of August 29, 2018 )

---

[11] Here we are departing from [3] which, in place of our $OD(a,b)$, made use of the predicate $(\exists\, x\,,\, y)\; [\,(2\,x+1)\,y = b \,\&\, a \geqslant y\,]$. Our slight change ensures, for every value of $v$, that $\varrho(v,u)$ holds only for finitely many $u$'s. It is also clear, for every value of $u$, that $\varrho(v,u)$ holds only for finitely many $v$'s.

[12] In particular, see [16, pp. 35–36, Exercise 8].

Detecting an exponential-growth Diophantine relation was a big challenge in 1968, when [3] was published; but our interest in potential rule-them-all equations rests, today, on the finite-fold-ness issue discussed in Sec. 1. The existence of a finite-fold Diophantine representation of exponentiation calls for the proof of a variant of the condition 2. of Theorem 6.7. Such a variant is presented in [12, p. 749]: we will check, below, that our $\varrho$ meets it, by figuring out integers $\alpha, \beta, \gamma, \delta$ exceeding 1 such that to each suitably large $w \in \mathbb{N}$ there correspond $u, v$ such that $\varrho(v, u)$, $u < \gamma\, w^{\beta}$, and $v > \delta\, \alpha^{w}$ hold.

Preliminary to Theorem 6.10, which will precisely state this, we prove a simple technical fact:

LEMMA 6.9. *For every real number $x \geqslant 1$, some positive* even *integer lies in the open interval $I_x := \,]\, 1 + \log_2(1+x)\,,\; 5 + 2\log_2 x\,[\,$.*

*Proof.* Since $1 + \log_2(1+x) > 1$ holds when $x \geqslant 1$, it is enough to prove that the width of $I_x$ exceeds 2, for every $x \geqslant 1$. This amounts to showing that the real-valued function $f(x) := 2 + 2\,\log_2 x - \log_2(1+x)$ only assumes, all over the open-ended interval $[1, +\infty[$, positive values. But this follows at once, considering that its derivative $f'$ satisfies the inequality

$$f'(x) \;\; = \;\; \tfrac{1}{\ln 2}\,\tfrac{x+2}{x^2+x} \;\; > \;\; 0$$

(implying that $f(x)$ is increasing), and that $f(1) = 1$. □

THEOREM 6.10. *Let $\alpha = 3^4$, $\beta = 2$, $\gamma = 2^7$, and $\delta = 3^3$. Then, to every $w \geqslant 1$ there correspond non-negative integers $u, v$ such that*

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

*Proof.* Recalling that

$$\varrho(v, u) \;\; := \;\; (\exists\, \ell)\,\big[\, v = y_{2^{2\,\ell+1}} \;\&\; 2^{2\,\ell+2} \mid u \;\; \& \;\; u \mid v\,\big]\,,$$

in order to prove the claim it is enough to show that, for every $w \geqslant 1$, there is an $\ell \in \mathbb{N}$ such that

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

Note that since $y_{i+1} \geqslant 3^i$ holds[13] for every $i$, we get $y_{2^{2\,\ell+1}} \geqslant 3^{2^{2\,\ell+1}-1}$ for every $\ell \in \mathbb{N}$. Our task hence further reduces to proving that, for every $w \geqslant 1$, there is an $\ell \in \mathbb{N}$ such that

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

---

[13] See entry 1. of the list of facts preceding Lemma A.1 in Appendix A.

namely

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

i.e.,

$$2^{2\,\ell} < 2^5\,w^2 \;\;\&\;\; 3^{2^{2\,\ell+1}} > 3^4 \cdot 3^{4\,w}\,. \tag{13}$$

Plainly, (13) is equivalent, for $w \geqslant 1$, to

$$2\,\ell < 5 + 2\,\log_2\,w \;\;\&\;\; 2^{2\,\ell+1} > 4 + 4\,w\,. \tag{14}$$

Since $2^{2\,\ell+1} > 4 + 4\,w$ is equivalent to

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

it turns out that (14) is equivalent, for $w \geqslant 1$, to

$$1 + \log_2(1+w) < 2\,\ell < 5 + 2\,\log_2\,w\,. \tag{15}$$

Hence, 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 (15). But this is an immediate consequence of the preceding lemma. □

Fact 5. *Pietro Corvaja (University of Udine) pointed out to us that the issue as to whether our quaternary quartic equation*

$$3 \cdot \left(r^2 + 3\,s^2\right)^2 - \left(u^2 + 3\,v^2\right)^2 \;\;=\;\; 2 \tag{†}$$

*has only finitely many solutions in* $\mathbb{N}$ *can be recast as the analogous problem concerning the system*

$$\left\{ \begin{array}{rcl} 3\,\xi^2 - \eta^2 & = & 2 \\ \xi\,\eta & = & \vartheta^2 + 3\,\nu^2 \end{array} \right. \tag{‡}$$

*over* $\mathbb{Z}$.

*In order to transform the solutions to* (‡) *into solutions to* (†)*, notice that* $\xi$ *and* $\eta$ *turn out to be coprime numbers; consequently, the representability of their product implies the representability of both of them.*

*The existence of finite-fold Diophantine representations for all listable sets thus reduces to the finitude of the set of integer points lying on a specific surface.*

## A. A conditional Diophantine representation of exponentiation

Following [18, pp. 442–443] rather faithfully, we shall now provide an existential definition,[14] *in terms of* the predicate $\varrho(v,u)$ introduced right before

[14] We refer here to the notion of *existential definability* as found in [6, p. 426], more general than the one originally provided in [18].

Lemma 6.4, of the triadic relation $b^n = c$. Specifically, we shall construct a formula

$$\varphi(\, b\,,\ n\,,\ c\,,\ z_1\,,\ldots,\ z_{16}\,)$$

that involves the shown variables, positive integer constants, addition, multiplication, the logical connectives $\mathscr{E}, \vee, \exists\,\nu, =$, and the predicate $\varrho$, so that the following biimplication holds all over $\mathbb{N}$, for $b \geqslant 1$ and $c \geqslant 1$:

$$b^n = c \quad\Longleftrightarrow\quad (\exists\, z_1\,,\ldots,\ z_{16})\ \varphi(\, b\,,\ n\,,\ c\,,\ z_1\,,\ldots,\ z_{16}\,)\,.$$

Accordingly,

$$\begin{aligned} b^n = c \quad\Longleftrightarrow\quad & \\ (\exists\, z_0\,,\ldots,\ z_{17})\Big[\Big(b = z_0 + 1\ \mathscr{E}\ c = z_{17} + 1\ \mathscr{E}\ \varphi(\, b\,,\ n\,,\ c\,,\ z_1\,,\ldots,\ z_{16}\,)\Big) & \\ \vee\quad (c-1)^2 + b + n = 0\quad\vee\quad c + b + (n - z_0 - 1)^2 = 0\Big] & \end{aligned}$$

will be the sought existential definition of exponentiation in terms of $\varrho$,[15] whence $\varrho$ can be eliminated (in terms of polynomial constructs) if $\mathcal{H}$ is true.[16] If this is the case, then it directly follows from the main result in [6] that every listable set is Diophantine.

We shall consider the sequence $\big\langle\langle \boldsymbol{x}_i(a)\,,\ \boldsymbol{y}_i(a)\rangle\big\rangle_{i\in\mathbb{N}}$ — of which we have treated so far the instance $\big\langle\langle x_i, y_i\rangle\big\rangle_{i\in\mathbb{N}} = \big\langle\langle \boldsymbol{x}_i(2)\,,\ \boldsymbol{y}_i(2)\rangle\big\rangle_{i\in\mathbb{N}}$ — such that $x = \boldsymbol{x}_i(a)\,,\ y = \boldsymbol{y}_i(a)$ is the $(i+1)$-st non-negative integer solution to the Pell equation

$$x^2 - (a^2 - 1)\, y^2 \quad = \quad 1 \quad \text{with} \quad a > 1\,.$$

Well-known facts about this sequence which we shall exploit are:

0. $\boldsymbol{y}_0(a) = 0\,,\ \ \boldsymbol{x}_0(a) = \boldsymbol{y}_1(a) = 1\,,\ \ \boldsymbol{x}_1(a) = a\,,$
   $\boldsymbol{y}_{i+2}(a) = 2\,a\,\boldsymbol{y}_{i+1}(a) - \boldsymbol{y}_i(a)$, and $\boldsymbol{x}_{i+2}(a) = 2\,a\,\boldsymbol{x}_{i+1}(a) - \boldsymbol{x}_i(a)\,;$
1. $(2\,a)^i \geqslant \boldsymbol{y}_{i+1}(a) > \boldsymbol{y}_{i+1}(a)/a > \boldsymbol{y}_i(a) \geqslant i$ and, moreover,
   $\boldsymbol{y}_{i+1}(a) \geqslant (2\,a - 1)^i$;
2. $\boldsymbol{x}_{i+1}(a) > \boldsymbol{x}_{i+1}(a)/a \geqslant \boldsymbol{x}_i(a) \geqslant a^i > i$ and, moreover,
   $a^{2\,i+2} \geqslant (2\,a)^{i+1} > \boldsymbol{x}_{i+1}(a),\ \ \boldsymbol{x}_{i+2}(a) > a^{i+2}$;

---

[15] An alternative technique, expounded in [19, p.112], enables one to express exponentiation in terms of $\varrho$ by making use of 13 outer existential variables instead of 18.

[16] One way of combining the second and third disjunct in the above specification of $b^n = c$ into a single-fold equation is: $b + \big((c-1)^2 + z_0\big)\, c + (n + c - z_0 - 1)^2 + \sum_{i=1}^{17} z_i = 0$.

3. $\boldsymbol{x}_i(a) - (a-b)\,\boldsymbol{y}_i(a) \equiv b^i \pmod{2\,a\,b - b^2 - 1}$;
4. $\boldsymbol{y}_i(a) \equiv i \pmod{a-1}$;
5. $(b \geqslant 1 \;\&\; a > b^n) \Longrightarrow [\, b^n = c \Longleftrightarrow c\,\boldsymbol{x}_n(a) \leqslant \boldsymbol{x}_n(a\,b) < (c+1)\,\boldsymbol{x}_n(a)\,]$;
6. $(b \geqslant 1 \;\&\; a > b^n) \Longrightarrow \left[\; \boldsymbol{x}_n(a) \leqslant \boldsymbol{x}_m(a\,b) < a\,\boldsymbol{x}_n(a) \iff m = n \;\right]$

(see, e.g., [18, pp. 439–440] and [11, pp. 527–528]).

The last two facts just recalled, namely 5. and 6., easily yield:

LEMMA A.1.

$$(b \geqslant 1 \;\&\; a > b^n) \Longrightarrow \left[\begin{array}{rcl} \boldsymbol{x}_n(a\,b) = u & \Longleftrightarrow & (\exists\, v)\Big(u^2 - (a^2\,b^2 - 1)\,v^2 = 1 \;\;\&\; \\ & & \qquad\qquad \boldsymbol{x}_n(a) \leqslant u < a\,\boldsymbol{x}_n(a)\Big) \end{array}\right];$$

$$(1 \leqslant c < a \;\&\; b \geqslant 1 \;\&\; a > b^n) \Longrightarrow \left[\begin{array}{l} b^n = c \Longleftrightarrow (\exists\, u\,,\, v)\Big(u^2 - (a^2\,b^2 - 1)\,v^2 = 1 \\ \qquad\qquad \;\&\;\; c\,\boldsymbol{x}_n(a) \leqslant u < (c+1)\,\boldsymbol{x}_n(a)\Big) \end{array}\right].$$

In preparation for the existential definition of $b^n = c$ in terms of our $\varrho$, we also need the following:

LEMMA A.2. *Suppose that $a > 1$, $a > n$, and $\boldsymbol{x}_a(a) > \ell$. Then,*

$$\ell \;=\; \boldsymbol{x}_n(a) \;\Longleftrightarrow\; (\exists\, s)\left[\ell^2 \;-\; (a^2 \;-\; 1)\left(n \;+\; (a \;-\; 1)\,s\right)^2 \;\;=\;\; 1\right].$$

*Proof.* (**'$\Longrightarrow$'**) Under the premises of the claim, if $\ell = \boldsymbol{x}_n(a)$ then we have $\ell^2 - (a^2-1)\left(\boldsymbol{y}_n(a)\right)^2 = 1$, where $\boldsymbol{y}_n(a) \equiv n \pmod{a-1}$ and $\boldsymbol{y}_n(a) \geqslant n$, so that $\boldsymbol{y}_n(a) = n + (a-1)\,s$ must hold for some $s$.

(**'$\Longleftarrow$'**) If $\ell \leqslant 1$, then $\ell^2 - (a^2-1)\left(n + (a-1)\,s\right)^2 = 1$ holds only for $\ell = 1$ and $n = s = 0$, in which case $\boldsymbol{x}_n(a) = \boldsymbol{x}_0(a) = 1 = \ell$.

If $\ell > 1 (= \boldsymbol{x}_0(a))$ and the premise of the claim is true, then the existence of an $s$ satisfying $\ell^2 - (a^2-1)\left(n + (a-1)\,s\right)^2 = 1$ yields that the equation $x^2 - (a^2-1)\,y^2 = 1$ has a solution $x = \ell = \boldsymbol{x}_i(a)$, $y = r = \boldsymbol{y}_i(a)$, where $i$ satisfies $1 \leqslant i < a$ and $\boldsymbol{y}_i(a) \equiv n \pmod{a-1}$. Observe that $\boldsymbol{y}_1(a), \ldots, \boldsymbol{y}_{a-1}(a)$ belong to different equivalence classes modulo $a-1$ because $\boldsymbol{y}_j(a) \equiv j \pmod{a-1}$ holds for $j = 1, \ldots, a-1$. Each of them satisfies $\boldsymbol{y}_j(a) \geqslant j$, and hence $\boldsymbol{y}_j(a) = j + (a-1)s_j$ for some $s_j \geqslant 0$. Thus the requirement $r = n + (a-1)\,s$ identifies the $r$ of interest uniquely: $i = n$ and, accordingly, $\ell = \boldsymbol{x}_n(a)$. □

Another key ingredient in our specification will be a special polynomial, which we get easily from [11, pp. 530–531]:[17]

LEMMA A.3. *There is a polynomial $Q$ with integer coefficients such that* (using $\tau = \square$ as a short for $\exists\, q\, (\, \tau = q^2\, )$)*:*

- $Q(w,h) = \square \implies h > w^w$*;*
- *to every $w$, there correspond $h$'s such that $Q(w,h) = \square$.*

*Proof.* Consider any $t > 2$. Since $(t^2-1)\,(t-1)^2$ is not a perfect square, the Pell equation

$$q^2 - (t^2-1)\,(t-1)^2\, z^2 \;=\; 1$$

in the unknowns $q$ and $z$ has infinitely many solutions

$$q \;=\; \boldsymbol{x}_i(t), \qquad (t-1)\, z \;=\; \boldsymbol{y}_i(t)\,,$$

each identified by a different value (divisible by $t-1$) of the subscript $i$.

In other words, for each $z > 0$ satisfying the equation

$$(t^2-1)\,(t-1)^2\, z^2 + 1 \;=\; \square\ , \tag{16}$$

$(t-1)\, z = \boldsymbol{y}_i(t)$ holds for some $i > 0$ such that $t-1 \mid i$. Hence $t-1 \leqslant i$, so that $\boldsymbol{y}_i(t) \geqslant \boldsymbol{y}_{t-1}(t)$ and therefore (since $t > 2$)

$$(t-1)\, z \;\geqslant\; (2\,t-1)^{t-2}\ . \tag{17}$$

Let us show that (16) yields

$$z - 1 \;>\; (t-3)^{t-3}\ . \tag{18}$$

In fact, if $t = 3$, then by (17) we have $2\, z \geqslant 5$ and therefore $z \geqslant 3$, which readily yields (18). On the other hand, if $t > 3$, then (17) implies

$$z \;>\; (2\,t-1)^{t-3} \;>\; (t-3)^{t-3}\ ,$$

again yielding (18).

Let $w$ and $h$ be such that $t = w+3$ and $z = h+1$; thus (16) becomes

$$(w+2)^3\,(w+4)\,(h+1)^2 + 1 \;=\; \square$$

and (18) implies $h > w^w$. In order to meet the conditions of the claim, it will hence suffice to put

$$Q(w,h) \;\coloneqq\; (w+2)^3\,(w+4)\,(h+1)^2 + 1\ .$$

(Notice that solving the equation $Q(w,h) = q^2$ amounts to solving the Pell equation $q^2 - [(w+3)^2 - 1]\,(w+2)^2\,(h+1)^2 = 1$.) □

---

[17] The predicate $Q(w,h) = \square$ which we shall now bring into play supersedes the one,

$$(\exists\, x\,,\ y)\,\big[x^2 - (w^2-1)\,(w-1)^2\, y^2 = 1\ \&\ x > 1\ \&\ w > 1\ \&\ h = w\, x\big]\,,$$

originally adopted in [18].

COROLLARY A.4. *Let $Q$ be as in Lemma A.3. For every $n$, $b$, and $c$, with $b \geqslant 1$ and $c \geqslant 1$, the conditions*

$$w > b \quad \& \quad w > n \quad \& \quad Q(w\,,\,h) = \square \quad \& \quad a \geqslant h \quad \& \quad a > c$$

*are satisfied by suitable positive integers $w, h, a$ and they imply*

$$b^n = c \quad \iff \quad (\exists\, u\,,\, v)\Big[ \quad u^2 = (a^2\, b^2 - 1)\, v^2 + 1 \quad \& \\ c\, \boldsymbol{x}_n(a) \quad \leqslant \quad u \quad < \quad (c+1)\, \boldsymbol{x}_n(a) \quad \Big].$$

*Proof.* To see that the stated conditions can be satisfied, pick arbitrarily a $w > b \max n$, then (exploiting Lemma A.3) take an $h$ such that $Q(w, h) = \square$ holds, and then take an $a \geqslant h \max (c+1)$. Thus $a \geqslant h > w^w \geqslant b^n$ will follow from the first condition in the claim of Lemma A.3, and we can exploit the second part of Lemma A.1. □

In view of what precedes, we can state that the following biimplication holds for $b \geqslant 1$ and $c \geqslant 1$ :

$$b^n = c \iff (\exists\, w, h, a, \ell, u, v, q)\Big( \ell = \boldsymbol{x}_n(a) \quad \& \\ w > b \ \max\ n \ \ \& \ Q(w\,,\,h) = q^2 \quad \& \\ a \geqslant h \ \max\,(c+1) \quad \& \ u^2 = (a^2\, b^2 - 1)\, v^2 + 1 \quad \& \\ c\, \ell \leqslant u < (c+1)\, \ell \Big)\,.$$

In light of it, if we now provided a Diophantine representation of the relation $\ell = \boldsymbol{x}_n(a)$, we would readily get that the relation $b^n = c$ is also Diophantine. However, as stated at the beginning of this section, we shall content ourselves with an existential definition of $b^n = c$ *in terms of* our $\varrho$.

As a matter of fact, $\varrho$ enables us to limit the size of $\ell$ as requested by Lemma A.2, by virtue of the implication

$$\big[\ell \leqslant d \,\&\, \varrho(d, a)\big] \quad \Longrightarrow \quad \ell < a^a < \boldsymbol{x}_a(a)\,.$$

(Here we are exploiting the implication $\varrho(d, a) \Longrightarrow d < a^a$ proved in Theorem 6.7; we are also instantiating the inequality $a^{i+2} < \boldsymbol{x}_{i+2}(a)$ — see entry 2. of the list of facts appearing before Lemma A.1 —, with $i = a - 2$ .)

There are infinitely many values of $a$ to which there corresponds a $d$ satisfying the condition $\varrho(d, a)\, \& d > \boldsymbol{x}_n(a)$; and, in order to specify exponentiation as is our aim here, we just need to define $\boldsymbol{x}_n(a)$ for a suitably large value of $a$. We hence get:

LEMMA A.5. *When $b \geqslant 1$ and $c \geqslant 1$, the following biimplication holds:*

$$
\begin{aligned}
b^n = c \iff (\exists\, w, h, a, d, \ell, s, u, v, q)\Big[\;& \ell \leqslant d \;\;\&\;\; \varrho(d,a) && \&\\
& \ell^2 = (a^2-1)\left(n + (a-1)\,s\right)^2 + 1 && \&\\
& w > b \max n \;\;\&\;\; Q(w\,,\,h) = q^2 \;\;\&\;\; a \geqslant h \max (c+1) && \&\\
& u^2 = (a^2\,b^2 - 1)\,v^2 + 1 && \&\\
& c\,\ell \leqslant u < (c+1)\,\ell \;\Big]\,.
\end{aligned}
$$

*Proof.* Let $b \geqslant 1$ and $c \geqslant 1$.

(‘$\Longleftarrow$’) Suppose that $w, h, a, d, \ell, s, u, v, q$ satisfy all constraints appearing on the right-hand side of the biimplication in the claim. Then it follows from $w > b \max n$ that $w \geqslant 2$; and, therefore, $a \geqslant h > w^w > 2^n > n$ and $a > 1$ hold. Moreover, $\ell \leqslant d < a^a < \boldsymbol{x}_a(a)$; hence, by Lemma A.2, we get $\ell = \boldsymbol{x}_n(a)$. Then, by means of the claim which follows Corollary A.4, we get $b^n = c$.

(‘$\Longrightarrow$’) Suppose that $b^n = c$. Choose $w$ and $h$ so that $w > b \max n$ and $Q(w,h) = \square$ hold. To every $k \geqslant n$ there correspond $a, d$ such that $\varrho(d,a)$ & $a^{2\,k} < d < a^a$; thus, clearly, $a \neq 0$ and $a \neq 1$, and hence $a > 2\,k \geqslant 2\,n \geqslant n$ and $\boldsymbol{x}_n(a) < \boldsymbol{x}_a(a)$, hold. Moreover, $\boldsymbol{x}_n(a) \leqslant \boldsymbol{x}_k(a) \leqslant (2\,a)^k \leqslant a^{2\,k} < d$; provided that $k \geqslant h \max c$, we also get $a > h \max c$.

Put $\ell = \boldsymbol{x}_n(a)$; then, by Lemma A.2, there is an $s$ such that $\ell^2 = (a^2 - 1)\left(n + (a-1)\,s\right)^2 + 1$; moreover, by Corollary A.4, there exist $u, v$ such that $u^2 = (a^2\,b^2 - 1)\,v^2 + 1$ and $c$ is the quotient of the integer division of $u$ by $\ell$. □

Summing up, we have:

$$
\begin{aligned}
b^n = c \iff (\exists\, w\,,\, h\,,\, a\,,\, d\,,\, \ell\,,\, s\,,\, u\,,\, v)\Big[\;& (c-1)^2 + b + n = 0 \vee\\
& (c + b = 0 \;\&\; n \geqslant 1) \;\vee\\
& \Big(b \geqslant 1 \;\;\&\;\; c \geqslant 1 \;\;\&\;\; \ell \leqslant d \;\;\&\;\; \varrho(d,a) && \&\\
& \ell^2 = (a^2-1)\left(n + (a-1)\,s\right)^2 + 1 && \&\\
& w > b \max n \;\;\&\;\; Q(w\,,\,h) = \square \;\;\&\;\; a \geqslant h \max (c+1) \;\;\&\\
& u^2 = (a^2\,b^2 - 1)\,v^2 + 1 \;\;\&\;\; c = \lfloor u/\ell \rfloor\Big) \;\Big]\,.
\end{aligned}
$$

To conclude, let us suppose that the assertion $\mathcal{H}$ stated in Sec. 5 is true. Theorem 6.7 then tells us that $\varrho(v,u)$ admits a polynomial Diophantine representation. As we have just ended reporting, a general scheme drawn from [18] enables us to get from that representation of $\varrho$ — which our supposition ensures to be *finite-fold*, see Fact 4 — a polynomial Diophantine representation of exponentiation: will this representation be finite-fold as well? Unfortunately not; in order to achieve finite-fold-ness, we should somewhat refine Julia Robinson's technique, so as to take advantage of specific features of our $\varrho$. Such features are the ones elicited in [12], which motivated us in developing Theorem 6.10 (and also footnote 11). We could not find in the literature any explicit instructions on how to exploit them, but a clue on how to proceed might come from a classical, concrete example of single-fold reduction of exponentiation to the triadic relation $y = \boldsymbol{y}_i(a)$, cf. [14, p.308] and [11, p.534ff.]: after [16, pp.31–32], we can cast that reduction as the biimplication

$$b^n = c \iff c = \left\lfloor \frac{\boldsymbol{y}_{n+1}(\,8\,b\,(n+1)\;\boldsymbol{y}_{n+1}(b+1)+2\,)}{\boldsymbol{y}_{n+1}(\,8\;\;(n+1)\;\boldsymbol{y}_{n+1}(b+1)\;\;\;\;)} \right\rfloor .$$

## B. Legendre symbols and their key properties

For an odd prime number $q$ and integer $a$, the *Legendre symbol* $\left(\frac{a}{q}\right)$ is defined as

$$\left(\frac{a}{q}\right) := \begin{cases} 0 & \text{if } q \mid a\,, \\ 1 & \text{if } q \nmid a \text{ and } a \text{ is a quadratic residue modulo } q\,, \\ -1 & \text{if } q \nmid a \text{ and } a \text{ is not a quadratic residue modulo } q. \end{cases}$$

Using *Euler's criterion*

$$\left(\frac{a}{q}\right) \equiv a^{\frac{q-1}{2}} \pmod{q}$$

one can easily compute Legendre symbols, since $\left(\frac{a}{q}\right) \in \{0,1,-1\}$.

Legendre symbols exhibit a *multiplicative* behavior:

$$\left(\frac{ab}{q}\right) = \left(\frac{a}{q}\right)\left(\frac{b}{q}\right),$$

for all integers $a, b$.

Finally, we mention the *quadratic reciprocity law*:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}},$$

with $q, p$ distinct odd primes.

For further information on Legendre symbols and their properties, the reader may refer to any introductory textbook on number theory (see, for instance, [8]).

## C. Correctness of the Descent Step

To prove the correctness of the Descent Step, we shall resort to the following result.

LEMMA C.1. *If $n$ is coprimely representable and $q > 3$ is a representable prime dividing $n$, then $n/q$ is coprimely representable.*

*Proof.* From the hypotheses, we have

$$\begin{aligned} n &= r^2 + 3\,s^2 \\ q &= u^2 + 3\,v^2\,, \end{aligned}$$

for pairs of coprime integers $r, s$ and $u, v$. Thus $q$ divides

$$\begin{aligned} u^2 n - r^2 q &= u^2(r^2 + 3\,s^2) - r^2(u^2 + 3\,v^2) \\ &= 3\,(s^2u^2 - r^2v^2) \\ &= 3\,(su + rv)(su - rv)\,, \end{aligned}$$

so that $q$ divides either $(su + rv)$ or $(su - rv)$, as $q > 3$. Let

$$t \coloneqq \mathsf{if}\ q \mid su - rv\ \mathsf{then}\ r\ \mathsf{else}\ -r\ \mathsf{endif}\,. \tag{19}$$

Then $q \mid su - tv$, and therefore $su - tv = dq$, for some integer $d$.

Let us show next that $u \mid t + 3\,dv$. This amounts to proving that $u \mid (t + 3\,dv)v$, as $u, v$ are coprime integers. We have:

$$\begin{aligned} (t + 3\,dv)v &= tv + 3\,dv^2 \\ &= su - dq + 3\,dv^2 \\ &= su - d\,(u^2 + 3\,v^2) + 3\,dv^2 \\ &= su - du^2\,. \end{aligned} \tag{20}$$

From $u \mid t + 3\,dv$, it follows

$$t = cu - 3\,dv\,, \tag{21}$$

for some integer $c$. In addition, by (20), $cuv = su - du^2$ holds. Thus $cv = s - du$ (as $u \neq 0$), i.e.,

$$s = cv + du\,. \tag{22}$$

Using the identity (1), we then have:

$$\begin{aligned} n = r^2 + 3\,s^2 = t^2 + 3\,s^2 &= (cu - 3\,dv)^2 + 3\,(cv + du)^2 \\ &= (u^2 + 3\,v^2)\,(c^2 + 3\,d^2) \\ &= (c^2 + 3\,d^2)\,q\,. \end{aligned}$$

Hence, $n/q = c^2 + 3\,d^2$ so it is representable. It only remains to show that $c, d$ are coprime. But this follows immediately from (21) and (22), since $r, s$ are coprime, and so, by (19), are $t, s$. Thus, $n/q$ is coprimely representable. □

LEMMA C.2 (Descent Step). *For a prime $p > 3$, if $p$ divides some coprimely representable integer, then $p$ is representable.*

*Proof.* Towards a contradiction, let us assume that the lemma does not hold and let $p$ be the smallest non-representable prime greater than 3 dividing some coprimely representable integer. Also, let $n = r^2 + 3\,s^2$ be the smallest coprimely representable integer divided by $p$, with $r, s$ coprime positive integers. We plainly have

$$p \nmid r \quad \text{and} \quad p \nmid s, \tag{23}$$

otherwise $p$ would divide both $r$ and $s$. In addition, we have

$$r < p/2 \quad \text{and} \quad s < p/2\,, \tag{24}$$

so that $n < p^2$ holds. Indeed, if $r > p/2$, then putting

$$r' \coloneqq |r - p|\,, \qquad d \coloneqq \gcd(r', s)\,, \qquad \bar{r} \coloneqq \frac{r'}{d}\,, \qquad \bar{s} \coloneqq \frac{s}{d}\,,$$

we would have

- $0 < \bar{r} < r$ and $0 < \bar{s} \leqslant s$, so that $\bar{r}^2 + 3\,\bar{s}^2 < n$;
- $\bar{r}$ and $\bar{s}$ are coprime, so $\bar{r}^2 + 3\,\bar{s}^2$ is coprimely representable;
- $p \mid \bar{r}^2 + 3\,\bar{s}^2$ (else $p \mid d$ and (23) would be contradicted).

But then the minimality of $n$ would be contradicted. Hence, $r < p/2$ must hold. Much in the same way, it can be shown that $s < p/2$ must hold as well.

From (24) and our assumption that $p$ is not representable (while $n$ is), it follows that

$$p < n = r^2 + 3\,s^2 < \frac{p^2}{4} + 3 \cdot \frac{p^2}{4} = p^2\,.$$

Hence, $1 < n/p < p$, and therefore all prime divisors of $n/p$ must be less than $p$.

We first rule out the possibility that $n/p$ has some prime divisor $q > 3$. Indeed, if this were the case, then, by the minimality of $p$, the prime $q$ would

be representable and therefore, by Lemma C.1, $n/q$ would be coprimely representable. But since $p \mid \frac{n}{q}$, the minimality of $n$ would be contradicted.

Likewise, we can show that $n$ must be odd. Indeed, if $2 \mid n$ then, by Lemma 4.3(a), $n/4$ would be representable and since $p \mid \frac{n}{4}$, the minimality of $n$ would again be contradicted.

Hence, by Lemma 4.3(b), the only possibility would be $n = 3\,p$. But then $3 \mid r$, so that $r = 3\,r_0$, for some integer $r_0$. Thus,

$$p \quad = \quad \frac{n}{3} \quad = \quad \frac{(3\,r_0)^2 + 3\,s^2}{3} \quad = \quad \frac{9\,r_0^2 + 3\,s^2}{3} \quad = \quad 3\,r_0^2 + s^2\,,$$

contradicting our initial assumption that $p$ is not representable.

Since in all cases we get a contradiction, the lemma is proved. □

## Acknowledgements

We are grateful to Martin Davis, who suggested the topic for this study and gave us encouragement throughout its development.

We had pleasant and profitable exchanges of ideas with Alberto Policriti and Pietro Corvaja (University of Udine), and with Luca Vallata. Prof. Corvaja, in particular, explained to us how to associate a candidate rule-them-all equation with each of the square-free rational integer $d > 1$ such that the ring of integers of $\mathbb{Q}(\sqrt{-d}\,)$ is an (imaginary, quadratic) unique-factorization domain; his advice enabled us to move on from the treatment of the discriminant $-3$ to the analogous treatments of $-2$ and $-11$.

The authors gratefully acknowledge partial support from project "STORAGE—Università degli Studi di Catania, Piano della Ricerca 2020/2022, Linea di intervento 2" and from the project FRA-UniTS (2016) "SCOMUNIKE: Statistical and COmputational Methods for UncertaiN and Incomplete KnowledgE".

### References

[1] P. Corvaja and J. Hančl, *A characterization of the honeycomb lattice*, unpublished manuscript (2011).

[2] D. A. Cox, *Primes of the form $x^2+ny^2$: Fermat, class field theory, and complex multiplication*, 2nd ed., Pure Appl. Math., Wiley, 2013.

[3] M. Davis, *One equation to rule them all*, Trans. New York Acad. Sci. Ser. II **30** (1968), no. 6, 766–773.

[4] M. Davis, Y. Matijasevič, and J. Robinson, *Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution*, Mathematical Developments Arising From Hilbert Problems (Providence, RI), Proceedings of Symposia in Pure Mathematics, vol. 28, American Mathematical Society, 1976, Reprinted in [20, p. 269ff.], pp. 323–378.

[5] M. Davis and H. Putnam, *A computational proof procedure; Axioms for number theory; Research on Hilbert's Tenth Problem*, Tech. Report AFOSR TR59-124, U.S. Air Force, October 1959, (Part III reprinted in [17, pp. 411-430]).
[6] M. Davis, H. Putnam, and J. Robinson, *The decision problem for exponential Diophantine equations*, Ann. of Math. (2) **74** (1961), no. 3, 425–436.
[7] O. Herrman, *A non-trivial solution of the Diophantine equation* $9(x^2+7y^2)^2 - 7(u^2+7v^2)^2 = 2$, Computers in Number Theory (A. O. L. Atkin and B. J. Birch, eds.), Academic Press, London, 1971, pp. 207–212.
[8] G. A. Jones and J. M. Jones, *Elementary number theory*, 1st ed., Springer Undergrad. Math. Ser., Springer, 1998.
[9] Y. I. Manin, *A course in mathematical logic*, Grad. Texts in Math., Springer, 1977.
[10] J. V. Matijasevič, *Enumerable sets are Diophantine*, Soviet Mathematics. Doklady **11** (1970), no. 3, 354–358, (Translated from [13]).
[11] Y. Matijasevič and J. Robinson, *Reduction of an arbitrary diophantine equation to one in 13 unknowns*, Acta Arith. **XXVII** (1975), 521–553, Reprinted in [20, p. 235ff.].
[12] Yu. V. Matiyasevich, *Towards finite-fold Diophantine representations*, J. Math. Sci. **171** (2010), no. 6, 745–752.
[13] Yu. V. Matiyasevich, *Diofantovost' perechislimykh mnozhestv*, Doklady Akademii Nauk SSSR **191** (1970), no. 2, 279–282, (Russian. Available in English translation as [10]; translation reprinted in [21, pp. 269–273]).
[14] 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** (1974), 77–93, (Russian. Translated into English as Y. V. Matiyasevich, Existence of noneffectivizable estimates in the theory of exponential Diophantine equations, *J. Soviet Math.* **8**, (1977), 299–311).
[15] Yu. V. Matiyasevich, *Martin Davis and Hilbert's tenth problem*, in Omodeo and Policriti [17], pp. 35–54.
[16] Yu. V. Matiyasevich, *Hilbert's tenth problem*, The MIT Press, Cambridge (MA) and London, 1993.
[17] E. G. Omodeo and A. Policriti (eds.), *Martin Davis on computability, computational logic, and mathematical foundations*, Outstanding Contributions to Logic, vol. 10, Springer, 2016.
[18] J. Robinson, *Existential definability in arithmetic*, Trans. Amer. Math. Soc. **72** (1952), no. 3, 437–449, Reprinted in [20, p. 47ff.].
[19] J. Robinson, *Diophantine decision problems*, Studies in Number Theory (W. J. LeVeque, ed.), Studies in Mathematics, vol. 6, Mathematical Association of America, 1969, pp. 76–116.
[20] J. Robinson, *The collected works of Julia Robinson*, Collected Works, vol. 6, Amer. Math. Soc., Providence, RI, 1996.
[21] G. E. Sacks (ed.), *Mathematical logic in the 20th century*, Singapore University Press; World Scientific Publishing Co., Inc., River Edge, NJ, 2003.
[22] D. Shanks, *Five number-theoretic algorithms*, Proceedings of the Second Manitoba Conference on Numerical Mathematics (University of Manitoba, Winnipeg,

Manitoba, 5–7 October) (R. S. D. Thomas and H. C. Williams, eds.), Congressus Numerantium, vol. VII, Utilitas Mathematica Publishing, Winnipeg, Manitoba, 1972, pp. 51–70.

[23] D. Shanks and S. S. Wagstaff, Jr., *48 more solutions of Martin Davis's quaternary quartic equation*, Math. Comp. **64** (1995), no. 212, 1717–1731.

Authors' addresses:

Domenico Cantone
Dipartimento di Matematica e Informatica
Università degli Studi di Catania
Viale Andrea Doria 6, 95125 Catania, Italy
E-mail: domenico.cantone@unict.it

Eugenio G. Omodeo
Dipartimento di Matematica e Geoscienze
Università degli Studi di Trieste
Via Valerio 12/1, 34127 Trieste, Italy
E-mail: eomodeo@units.it

Received May 27, 2021
Revised December 19, 2021
Accepted December 19, 2021