Further reflections on candidate “rule-them-all” equations [1]

Domenico Cantone, Eugenio G. Omodeo

Università degli Studi di Trieste

Dip. Matematica e Geoscienze — DMI

JAF 37 May 28, 2018 Firenze

Work funded by: (1) INdAM/GNCS 2017 “DECORE: DEClarative approach for Object REconstruction”; (2) FRA-UniTS 2016 “SCOMUNIKE: Statistical and COmputational Methods for UncertaiN and Incomplete KnowledgE”.

MEMORANDUM
RM-5494-PR
FEBRUARY 1968

ONE EQUATION TO RULE THEM ALL

Martin Davis

PREPARED FOR:
UNITED STATES AIR FORCE PROJECT RAND

The RAND Corporation
SANTA MONICA • CALIFORNIA

DIVISION OF MATHEMATICS

ONE EQUATION TO RULE THEM ALL*

Martin Davis

Mathematics Department, New York University, New York, N.Y.

Let H stand for the assertion:
The equation

$$9\left(u^2 + 7v^2\right)^2 - 7\left(r^2 + 7s^2\right)^2 = 2 \tag{1}$$

has no solution in non-negative integers except the trivial $u = r = 1$, $v = s = 0$.

We must leave the truth of H open; however, in this note we shall prove:

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

As will be seen our methods yield a considerably stronger result. Also, the reader will see how the methods used can be readily adapted to obtain various other hypotheses about which the same can be demonstrated as we do here for H. We will conclude with a report on numerical calculations (some using the JOSS system) seeking counterexamples to H.

We wish to acknowledge helpful discussions with Robert DiPaola, Oliver Gross, Hilary Putnam, Norman Shapiro, and Joel Spencer. The ideas of Section 3 come from unpublished joint work done with Hilary Putnam during the summer of 1960.‡

1. SOME PROPERTIES OF SOLUTIONS OF THE PELL EQUATION $x^2 - 7y^2 = 1$

Below, p always is a prime number.

Lemma 1. The successive non-negative integer solutions of $x^2 - 7y^2 = 1$ are given (for $n \geq 0$) by

$$x_n + y_n\sqrt{7} = (8 + 3\sqrt{7})^n$$

Proof. By Theorem 104 of Reference 8, we have:

*This paper was presented at a meeting of the Division on March 7, 1968.
†The research in this paper was partly sponsored by the Air Force Office of Scientific Research and was partly conducted while the author was a consultant for the RAND Corporation. "JOSS" is the RAND Corporation's trademark for its computing system. For previous results and general background, see Chapter 7 of Reference 1, and References 2-9.
‡The same material is referred to as "Proposition 2" in Reference 3. As stated, the "proposition" requires the correction: Replace "$r^2 + ds^2$" by "$a_1 a_1'(r^2 + ds^2)$."

766

Outline

1. *Existentially definable*, in particular *Diophantine*, sets
   - single-fold and finite-fold existential representations
2. Relations of *exponential growth*
3. Quaternary quartic "rule-them-all" equations. E.g., over $\mathbb{N}$:
   $3\ \left(r^2+3\,s^2\right)^2-\left(u^2+3\,v^2\right)^2\ =\ 2$
4. - Integers expressible in a specific quadratic form, e.g. $u^2+3\,v^2$
   - A novel quaternary quartic (over $\mathbb{Z}$):
     $11\ \left(s^2+s\,r+3\,r^2\right)^2-\left(v^2+v\,u+3\,u^2\right)^2\ =\ 2$
5. Is the exponential-growth relation

$$\left\{\langle u, \boldsymbol{y}_{2^{2\,\ell+1}}(11)\rangle\ :\ \ell\geqslant 2\ \&\ u\geqslant 2^{2\,\ell+2}\right\}$$

Diophantine?

Outline

1. *Existentially definable*, in particular *Diophantine*, sets
   - single-fold and finite-fold existential representations

Outline

2. Relations of *exponential growth*

3. Quaternary quartic "rule-them-all" equations. E.g., over $\mathbb{N}$:
$$3\ \left(r^2+3\,s^2\right)^2-\left(u^2+3\,v^2\right)^2 \quad = \quad 2$$

Outline

4. - Integers expressible in a specific quadratic form, e.g. $u^2 + 3\,v^2$

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

- A novel quaternary quartic (over $\mathbb{Z}$):
  $11\left(s^2+s\,r+3\,r^2\right)^2-\left(v^2+v\,u+3\,u^2\right)^2\;=\;2$

Outline

5. Is the exponential-growth relation

$$\left\{ \langle u, \boldsymbol{y}_{2^{2\,\ell+1}}(11) \rangle \ : \ \ell \geqslant 2 \ \& \ u \geqslant 2^{2\,\ell+2} \right\}$$

Diophantine?

Outline

1. *Existentially definable*, in particular *Diophantine*, sets
   - single-fold and finite-fold existential representations
2. Relations of *exponential growth*
3. Quaternary quartic “rule-them-all” equations. E.g., over $\mathbb{N}$:
   $$3\;\left(r^2+3\,s^2\right)^2-\left(u^2+3\,v^2\right)^2 \;=\; 2$$
4. - Integers expressible in a specific quadratic form, e.g. $u^2+3\,v^2$
   - A novel quaternary quartic (over $\mathbb{Z}$):
     $$11\;\left(s^2+s\,r+3\,r^2\right)^2-\left(v^2+v\,u+3\,u^2\right)^2 \;=\; 2$$
5. Is the exponential-growth relation

$$\left\{\langle u, \boldsymbol{y}_{2^{2\,\ell+1}}(11)\rangle \;:\; \ell \geqslant 2 \;\&\; u \geqslant 2^{2\,\ell+2}\right\}$$

Diophantine? $\boxed{11\,y^2+1=\square}$

The finite-fold-ness issue

A relation $\mathcal{R} \subseteq \mathbb{N}^n$ is said to be ***existentially definable in terms of some relation*** $\mathcal{J}(\bullet, \ldots, \bullet)$ iff

$$\mathcal{R}(a_1, \ldots, a_n) \iff$$

$$(\exists x_1 \cdots \exists x_m)\, \varphi(\, a_1, \ldots, a_n \,,\, x_1, \ldots, x_m \,)$$

holds, over $\mathbb{N}$, for some formula φ that only involves :

A relation $\mathcal{R} \subseteq \mathbb{N}^n$ is said to be ***existentially definable in terms of some relation*** $\mathcal{J}(\bullet, \ldots, \bullet)$ iff

$$\mathcal{R}(a_1, \ldots, a_n) \iff$$

$$(\exists x_1 \cdots \exists x_m)\, \varphi(\overbrace{\underbrace{a_1, \ldots, a_n}_{\text{parameters}}, \underbrace{x_1, \ldots, x_m}_{\text{unknowns}}}^{\text{variables}})$$

holds, over $\mathbb{N}$, for some formula φ that only involves :

- the shown variables,
- positive integer constants,

A relation $\mathcal{R} \subseteq \mathbb{N}^n$ is said to be ***existentially definable in terms of some relation*** $\mathcal{J}(\bullet, \ldots, \bullet)$ iff

$$\mathcal{R}(a_1, \ldots, a_n) \iff (\exists x_1 \cdots \exists x_m)\, \varphi(\overbrace{\underbrace{a_1, \ldots, a_n}_{\text{parameters}}, \underbrace{x_1, \ldots, x_m}_{\text{unknowns}}}^{\text{variables}})$$

holds, over $\mathbb{N}$, for some formula φ that only involves :

- addition, multiplication,
- the logical connectives $\&$, $\vee$, $\exists x$, $=$

A relation $\mathcal{R} \subseteq \mathbb{N}^n$ is said to be ***existentially definable in terms of some relation*** $\mathcal{J}(\bullet, \ldots, \bullet)$ iff

$$\mathcal{R}(a_1, \ldots, a_n) \iff (\exists x_1 \cdots \exists x_m)\, \varphi(\overbrace{\underbrace{a_1, \ldots, a_n}_{\text{parameters}}, \underbrace{x_1, \ldots, x_m}_{\text{unknowns}}}^{\text{variables}})$$

holds, over $\mathbb{N}$, for some formula φ that only involves :

- the shown variables,
- positive integer constants,
- addition, multiplication,
- the logical connectives $\&$, $\vee$, $\exists x$, $=$, and
- $\boxed{\text{a predicate for } \mathcal{J}}$.

A relation $\mathcal{R} \subseteq \mathbb{N}^n$ is said to be ***existentially definable in terms of some relation*** $\mathcal{J}(\bullet, \ldots, \bullet)$ iff

$$\mathcal{R}(a_1, \ldots, a_n) \iff (\exists x_1 \cdots \exists x_m)\, \varphi(\overbrace{\underbrace{a_1, \ldots, a_n}_{\text{parameters}}, \underbrace{x_1, \ldots, x_m}_{\text{unknowns}}}^{\text{variables}})$$

holds, over $\mathbb{N}$, for some formula φ that only involves :

- the shown variables,
- positive integer constants,
- addition, multiplication,
- the logical connectives $\&$, $\vee$, $\exists x$, $=$, and
- $\boxed{\text{a predicate for } \mathcal{J}}$.

When $\mathcal{J}$ is absent, $\mathcal{R}$ is also called ***Diophantine***.

Single-fold existential definitions

An existential definition

$$\exists \vec{x} \quad \varphi(\, \vec{a},\, \vec{x}\,)$$

(as above) is said to be ***single-fold*** if

$$\forall \vec{a}\, \forall \vec{x}\, \forall \vec{y} \Big[\quad \varphi(\, \vec{a},\, \vec{x}\,) \ \&\ \varphi(\, \vec{a},\, \vec{y}) \implies \vec{x} = \vec{y} \quad \Big]$$

(i.e., $\varphi(\, a_1, \ldots, a_n\,,\, x_1, \ldots, x_m\,)$ never has multiple solutions).

Singlefold-ness

Single-fold existential definitions

An existential definition

$$\exists\, \vec{x} \quad \varphi(\, \vec{a},\, \vec{x}\,)$$

(as above) is said to be ***single-fold*** if

$$\forall\, \vec{a}\, \forall\, \vec{x}\, \forall\, \vec{y} \Big[\quad \varphi(\, \vec{a},\, \vec{x}\,) \;\&\; \varphi(\, \vec{a},\, \vec{y}) \implies \vec{x} = \vec{y} \quad\Big]$$

(i.e., $\varphi(\, a_1, \ldots, a_n\, ,\, x_1, \ldots, x_m\,)$ never has multiple solutions).

Finite-fold existential definitions

The definition of ***finite-fold***-ness is akin:

To each $\vec{a}$ there must correspond a *finite* number of solutions.

Now consider listable[2] (aka effectively enumerable) sets.

[2] **Def.** A set is *listable* if its elements can be generated exhaustively by an algorithmic (perhaps non-terminating) procedure.

Two important theorems
(Davis, Putnam, Robinson, Matiyasevich)

DPR theorem (See [DPR61])

Each listable set is *existentially definable in terms of exponentiation* (which is the rel. consisting of all triples $\langle b, n, c\rangle$ such that $b^n = c$).

(One can also choose any fixed $b \geqslant 2$)

[2] **Def.** A set is *listable* if its elements can be generated exhaustively by an algorithmic (perhaps non-terminating) procedure.

Two important theorems
(Davis, Putnam, Robinson, Matiyasevich)

DPR theorem (See [DPR61])

Each listable set is *existentially definable in terms of exponentiation* (which is the rel. consisting of all triples $\langle b, n, c\rangle$ such that $b^n = c$).

(One can also choose any fixed $b \geqslant 2$)

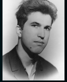
Significant improvement to DPR (see [Mat74], [JM84])

Each listable set admits an existential *single-fold* repr'tion in terms of exponentiation.

(See also [Dav93])

[2] **Def.** A set is *listable* if its elements can be generated exhaustively by an algorithmic (perhaps non-terminating) procedure.

Open p.: Does exponentiation admit a single-fold (or at least finite-fold) Diophantine definition ?



"After the DPR-theorem was proved in 1961, in order to establish the existence of Diophantine representations for *every* effectively enumerable set it was sufficient to find a Diophantine representation for *one particular* set of triples

$$\{ \langle a, b, c \rangle \quad | \quad a = b^c \} \ . \tag{12}$$

Today we are in a similar position with respect to single-fold (and finite-fold) Diophantine representations: now that we can construct single-fold exponential Diophantine representations for all effectively enumerable sets, in order to transform them into single-fold (or finite-fold) genuinely Diophantine representations, it would be sufficient to find a single-fold (or, respectively, finite-fold) Diophantine representation for the same set of triples (12) $\cdots$"

[Mat10, p. 748]

Relations of exponential growth

From now on, $\mathcal{J}$ will designate a relation such that

Dyadic exponential-growth relations

From now on, $\mathcal{J}$ will designate a relation such that

1. $\mathcal{J}(u,v) \implies v < u^u$;
2. $\forall\, \ell\, (\exists\, u\,,\; v)\big[\, \mathcal{J}(\,u\,,\; v\,)\;\&\; u^{\ell} < v\,\big]$.

After [Rob52], such a relation is said to be of ***exponential growth***.

From now on, $\mathcal{J}$ will designate a relation such that

1. $\mathcal{J}(u, v) \implies v < u^u$;
2. $\forall \ell\, (\exists\, u, v)\big[\, \mathcal{J}(u, v)\ \&\ u^\ell < v \,\big]$.

After [Rob52], such a relation is said to be of ***exponential growth***.

Historical example — ⌣ Diophantine! ⌣

Take

$$\mathcal{J} = \big\{ \langle u, F_{2u} \rangle \mid u > 1 \big\} ,$$

where

$$F_0 = 0 , \quad F_1 = 1 , \quad F_{\ell+2} = F_{\ell+1} + F_\ell ,$$

for $\ell = 0, 1, 2, \ldots$ (See [Mat70b])

Diophantine reduction of exponentiation to <u>any</u> $\mathcal{J}$ of exponential growth [Rob52]

$$
\begin{aligned}
& b^n = c \iff (\exists\, w,\, h,\, a,\, d,\, \ell,\, u,\, v,\, s,\, q,\, z)\Big[\\
& (c-1)^2 + b + n = 0 \;\vee\; c + b + (n - z - 1)^2 = 0 \;\vee \\
& \Big(b \geqslant 1 \;\&\; c = z + 1 \\
& \quad \&\; w > b \;\&\; w > n \;\&\; \boxed{Q(w,\, h) = q^2} \;\&\; a \geqslant h \;\&\; a > c \\
& \quad \&\; u^2 = (a^2\, b^2 - 1)\, v^2 + 1 \;\&\; \ell \leqslant d \;\&\; \lfloor c = u/\ell \rfloor \\
& \quad \&\; \ell^2 = (a^2 - 1)\,\big(n + (a-1)\, s\big)^2 + 1 \;\&\; \boxed{\boxed{\mathcal{J}(a, d)}} \Big)\Big]
\end{aligned}
$$

$$b^n = c \iff (\exists\, w, h, a, d, \ell, u, v, s, q, z)\Big[$$
$$(c-1)^2 + b + n = 0 \;\vee\; c + b + (n - z - 1)^2 = 0 \;\vee$$
$$\Big(b \geqslant 1 \;\&\; c = z + 1$$
$$\&\; w > b \;\&\; w > n \;\&\; \boxed{Q(w, h) = q^2} \;\&\; a \geqslant h \;\&\; a > c$$
$$\&\; u^2 = (a^2\, b^2 - 1)\, v^2 + 1 \;\&\; \ell \leqslant d \;\&\; \lfloor c = u/\ell \rfloor$$
$$\&\; \ell^2 = (a^2 - 1)\,\big(n + (a-1)\, s\big)^2 + 1 \;\&\; \boxed{\boxed{\mathcal{J}(a, d)}}\Big)\Big]$$

Here:

1. $Q(x, y) = \square \implies y > x^x$;
2. $\forall x\, \exists y \quad Q(x, y) = \square$;

(See [MR75])

$$
\begin{aligned}
b^n = c \iff (\exists\, w, h, a, d, \ell, u, v, s, q, z)\Big[\\
&(c-1)^2 + b + n = 0 \;\vee\; c + b + (n - z - 1)^2 = 0 \;\vee\\
&\Big(b \geqslant 1 \;\&\; c = z + 1\\
&\quad \&\; w > b \;\&\; w > n \;\&\; \boxed{Q(w, h) = q^2} \;\&\; a \geqslant h \;\&\; a > c\\
&\quad \&\; u^2 = (a^2\, b^2 - 1)\, v^2 + 1 \;\&\; \ell \leqslant d \;\&\; \lfloor c = u/\ell \rfloor\\
&\quad \&\; \ell^2 = (a^2 - 1)\,\big(n + (a-1)\, s\big)^2 + 1 \;\&\; \boxed{\boxed{\mathcal{J}(a, d)}}\Big)\Big]
\end{aligned}
$$

Here:

1. $Q(x, y) = \Box \implies y > x^x$;
2. $\forall x\, \exists y \quad Q(x, y) = \Box$;

e.g., $Q \leftrightharpoons (x+2)^3\,(x+4)\,(y+1)^2 + 1$. (See [MR75])

Davis's quaternary quartic equation and its siblings

How many solutions has Davis's eq. $9\left(u^2+7v^2\right)^2-7\left(r^2+7s^2\right)^2 = 2$?

[Dav68] takes into account the sequence

$$\langle y_i \rangle_{i\in\mathbb{N}} = \langle 0, 3,\ 48,\ 640, \dots \rangle,$$

such that y_i is the $(i+1)$-st solution of the Pell equation

$$7\,y^2+1 = \square\ .$$

[Dav68] takes into account the sequence

$$\langle y_i \rangle_{i\in\mathbb{N}} = \langle 0, 3,\ 48,\ 640, \ldots \rangle ,$$

such that y_i is the $(i+1)$-st solution of the Pell equation

$$7\,y^2+1 = \square\,.$$

Through the study of integers expressible in the form $u^2+7\,v^2$, Davis proves that the exponential-growth relation

$$\left\{ \langle u\,,\ y_{2^\ell} \rangle\ :\ \ell \geqslant 0\ \&\ u \geqslant 2^\ell\ \&\ u > 16 \right\}$$

is *Diophantine* $\boxed{\textbf{if}}$ the equation

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

has no solution in $\mathbb{N}$ except the trivial one: $u=r=1\,,\ v=s=0\,.$

$$9\ \left(u^2+7\,v^2\right)^2-7\ \left(r^2+7\,s^2\right)^2\ =\ 2\ \ ?$$

[Dav68] takes into account the sequence

$$\boldsymbol{y}(7)\quad=\quad\langle y_i\rangle_{i\in\mathbb{N}}\quad=\quad\langle 0,3,\ 48,\ 640,\ldots\rangle\,,$$

such that y_i is the $(i+1)$-st solution of the Pell equation

$$7\,y^2+1\quad=\quad\Box\ .$$

Through the study of integers expressible in the form $u^2+7\,v^2$, Davis proves that the exponential-growth relation

$$\left\{\langle u\,,\ y_{2^\ell}\rangle\ :\ \ell\geqslant 0\ \&\ u\geqslant 2^\ell\ \&\ u>16\right\}$$

$$\boxed{\boldsymbol{y}_{2^\ell}(7)}$$

is *Diophantine* **if** the equation

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

has no solution in $\mathbb{N}$ except the trivial one: $u=r=1\,,\ v=s=0\,.$

How many solutions has Davis's eq.

$$9\ \left(u^2+7\,v^2\right)^2-7\ \left(r^2+7\,s^2\right)^2\ =\ 2\ \text{?}$$

Nontrivial solutions exist [SW95]... ☹ ☺ ... Even so:

From [DMR76]: "It can be shown that a *singlefold* Diophantine representation of $a = 2^c$ can be constructed if the equation

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

has only a *finite number* of solutions."

Upon Martin D.'s suggestion, we sought other candidates to the role of

$$\boxed{\textit{`rule-them-all' equation}}$$

Upon Martin D.'s suggestion, we sought other candidates to the role of

$\boxed{\textit{`rule-them-all' equation}}$

Today there are four (potentially eight) competitors:

- -2 $\quad 2\,(r^2+2\,s^2)^2-(u^2+2\,v^2)^2 \;=\; 1$
- -3 $\quad 3\,(r^2+3\,s^2)^2-(u^2+3\,v^2)^2 \;=\; 2$
- -7 $\quad 9\,(u^2+7\,v^2)^2-7\,(r^2+7\,s^2)^2 \;=\; 2$
- -11 $\quad 11\,(r^2+r\,s+3\,s^2)^2-(v^2+v\,u+3\,u^2)^2 \;=\; 2$ (over $\mathbb{Z}$)

Each of these stems from a square-free rational integer $d>1$ such that the integers of $\mathbb{Q}(\sqrt{-d})$ form a unique-factorization domain.

Solutions to our candidate rule-them-all eq's

Trivial solutions

A solution in $\mathbb{N}$, for each of the four candidates, is:

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

When the discriminant is -11, the trivial solutions in $\mathbb{Z}$ are:
$s = 0$, $r \in \{-1, 1\}$ and either $v = 0$, $u \in \{-1, 1\}$ or $u = 1$, $v = -1$.

Non-trivial solutions (in $\mathbb{N}$)

At least 50 solutions were found for the discriminant -7.
Two non-trivial solutions for the discriminant -3 were detected, and kindly communicated to us, by Boris Z. Moroz (Rheinische Friedrich-Wilhelms-Universität Bonn) and Carsten Roschinski:

$$\begin{array}{cccc} r = 16\,, & s = 25\,, & u = 4\,, & v = 35\,; \\ r = 124088\,, & s = 7307\,, & u = 134788\,, & v = 54097\,. \end{array}$$

Integers representable in the form $\upsilon^2 + \upsilon\, u + 3\, u^2$

To each of our discriminants

$$-2\,,\quad -3\,,\quad -7\,,\quad -11\,,$$

there corresponds a notion of *representable number*; to wit, a positive integer which can be written in the respective quadratic form:

- -2 $u^2 + 2\,v^2$
- -3 $u^2 + 3\,v^2$
- -7 $u^2 + 7\,v^2$
- -11 $\boxed{v^2 + v\,u + 3\,u^2}$

with $u\,,\,v \in \mathbb{Z}$.

To each of our discriminants

$$-2\,, \quad -3\,, \quad -7\,, \quad -11\,,$$

there corresponds a notion of $\boxed{\textit{representable number}}$; to wit, a positive integer which can be written in the respective quadratic form:

- -2 $u^2 + 2\,v^2$
- -3 $u^2 + 3\,v^2$
- -7 $u^2 + 7\,v^2$
- -11 $\boxed{v^2 + v\,u + 3\,u^2}$

with $u\,,\,v \in \mathbb{Z}$.

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

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

Call a prime number p *poison* if one of the following congruences holds:

$$p \equiv 2\,,\ 6\,,\ 7\,,\ 8\,,\ 10 \pmod{11}\,.$$

Primes of the form $\upsilon^2 + \upsilon\, u + 3\, u^2$

Every *non*-poison prime is so representable

Positive integers of the form $\upsilon^2 + \upsilon\, u + 3\, u^2$

A positive integer x is so representable if and only if there is *no* poison prime dividing it to an odd power

Now consider the increasing sequence $\langle y_i \rangle_{i \in \mathbb{N}} = \langle 0, 3, 60, 1197, \ldots \rangle$ of all solutions to the equation

$$11\, y^2 + 1 \quad = \quad \square \; .$$

Then

Now consider the increasing sequence $\langle y_i \rangle_{i \in \mathbb{N}} = \langle 0, 3, 60, 1197, \ldots \rangle$ of all solutions to the equation

$$11\, y^2 + 1 \quad = \quad \Box\ .$$

Then

- y_{2^h}, with $h > 0$, is representable as $\upsilon^2 + \upsilon\, u + 3\, u^2$ iff $2 \nmid h$

Now consider the increasing sequence $\langle y_i \rangle_{i \in \mathbb{N}} = \langle 0, 3, 60, 1197, \ldots \rangle$ of all solutions to the equation

$$11\, y^2 + 1 \quad = \quad \square \; .$$

Then (denoting by $\langle x_i \rangle_{i \in \mathbb{N}}$ the associated seq. $\langle 1, 10, 199, 3970, \ldots \rangle$):

- if $y_{2^\ell\,(2\,h+1)}$ is representable, so are $\overbrace{3\, x_h + 11\, y_h \text{ and } x_h + 3\, y_h}^{\textit{coprime}}$

Now consider the increasing sequence $\langle y_i \rangle_{i \in \mathbb{N}} = \langle 0, 3, 60, 1197, \ldots \rangle$ of all solutions to the equation

$$11\, y^2 + 1 \quad = \quad \square \;.$$

Then (denoting by $\langle x_i \rangle_{i \in \mathbb{N}}$ the associated seq. $\langle 1, 10, 199, 3970, \ldots \rangle$):

- if $y_{2^\ell\,(2\,h+1)}$ is representable, so are $\overbrace{3\, x_h + 11\, y_h \text{ and } x_h + 3\, y_h}^{\textit{coprime}}$
- if y_n is representable for some $n > 0$ *not* a power of 2, then the system
$$\begin{cases} X^2 - 11\, Y^2 & = & 1\,, \\ 3\, X + 11\, Y & = & \upsilon^2 + \upsilon\, u + 3\, u^2\,, \\ X + \;\; 3\, Y & = & r^2 + r\, s + 3\, s^2 \end{cases}$$
has a solution in $\mathbb{N}$ for which $Y \neq 0$

Now consider the increasing sequence $\langle y_i \rangle_{i \in \mathbb{N}} = \langle 0, 3, 60, 1197, \ldots \rangle$ of all solutions to the equation

$$11\, y^2 + 1 \quad = \quad \Box\ .$$

Then (denoting by $\langle x_i \rangle_{i \in \mathbb{N}}$ the associated seq. $\langle 1, 10, 199, 3970, \ldots \rangle$):

- y_{2^h}, with $h > 0$, is representable as $\upsilon^2 + \upsilon\, u + 3\, u^2$ iff $2 \nmid h$
- if $y_{2^\ell\,(2\,h+1)}$ is representable, so are $\overbrace{3\, x_h + 11\, y_h \text{ and } x_h + 3\, y_h}^{\textit{coprime}}$
- if y_n is representable for some $n > 0$ *not* a power of 2, then the system

$$\begin{cases} X^2 - 11\, Y^2 & = & 1\,, \\ 3\, X + 11\, Y & = & \upsilon^2 + \upsilon\, u + 3\, u^2\,, \\ X + \ 3\, Y & = & r^2 + r\, s + 3\, s^2 \end{cases}$$

  has a solution in $\mathbb{N}$ for which $Y \neq 0$; $\therefore$, the eq.

$$11\, \left(r^2 + r\, s + 3\, s^2\right)^2 - \left(\upsilon^2 + \upsilon\, u + 3\, u^2\right)^2 \quad = \quad 2$$

  has a solution with either

$$r^2 + r\, s + 3\, s^2 \neq 1 \ \text{ or } \upsilon^2 + \upsilon\, u + 3\, u^2 \neq 3\,.$$

Now consider the increasing sequence $\langle y_i\rangle_{i\in\mathbb{N}} = \langle 0,3,60,1197,\ldots\rangle$ of all solutions to the equation

$$11\,y^2+1 \quad = \quad \square\ .$$

Then (denoting by $\langle x_i\rangle_{i\in\mathbb{N}}$ the associated seq. $\langle 1,10,199,3970,\ldots\rangle$):

- if $y_{2^\ell\,(2\,h+1)}$ is representable, so are $\overbrace{3\,x_h+11\,y_h \text{ and } x_h+3\,y_h}^{\textit{coprime}}$
- if y_n is representable for some $n>0$ *not* a power of 2, then the system

$$\begin{cases} X^2-11\,Y^2 &= \ 1\,, \\ 3\,X+11\,Y &= \ \upsilon^2+\upsilon\,u+3\,u^2\,, \\ X+\ 3\,Y &= \ r^2+r\,s+3\,s^2 \end{cases}$$

has a solution in $\mathbb{N}$ for which $Y\neq 0$; $\therefore$, the eq.

$$11\ \left(r^2+r\,s+3\,s^2\right)^2-\left(\upsilon^2+\upsilon\,u+3\,u^2\right)^2 \quad = \quad 2$$

has a solution such that

$$\left(r^2+r\,s+3\,s^2\right)\ \left(\upsilon^2+\upsilon\,u+3\,u^2\right) \mid y_n\ .$$

Is
$\left\{\langle u, y_{2^{2\ell+1}}\rangle \ : \ell \geqslant 2 \;\&\; u \geqslant 2^{2\ell+2}\right\}$
a Diophantine set?

An exponential-growth relation

Consider the relation

$$OD(a,\ b) \quad \overset{}{\Longleftrightarrow}_{\mathsf{Def}} \quad (\exists\, x)\big[\,(2\,x+1)\,a = b\,\big]\ .$$

Consider the relation

$$OD(a,\ b) \quad \Longleftrightarrow_{\mathrm{Def}} \quad (\exists\, x)\big[\,(2\,x+1)a = b\,\big]\ .$$

Then:

- $OD(\,u\,,\ y_{2^{2\,\ell+1}}\,) \quad \Longleftrightarrow \quad u \geqslant 2^{2\,\ell+2}\ \&\ u \mid y_{2^{2\,\ell+1}}$,
- the relation

  $$\mathcal{J}(\,u\,,\ w\,) \quad \Longleftrightarrow_{\mathrm{Def}} \quad w \in \{y_{2^{2\,\ell+1}} : \ell \geqslant 2\}\ \&\ OD(\,u\,,\ w\,)$$

  has exponential growth.

Consider the relation

$$OD(a,\ b) \quad \Longleftrightarrow_{\mathrm{Def}} \quad (\exists\, x)\big[\,(2\,x+1)a = b\,\big]\ .$$

Then:

- $OD(\,u\,,\ y_{2^{2\,\ell+1}}\,) \quad \Longleftrightarrow \quad u \geqslant 2^{2\,\ell+2}\ \&\ u \mid y_{2^{2\,\ell+1}}\ ,$
- the relation
  $$\mathcal{J}(\,u\,,\ w\,) \quad \Longleftrightarrow_{\mathrm{Def}} \quad w \in \{y_{2^{2\,\ell+1}}\ :\ \ell \geqslant 2\}\ \&\ OD(\,u\,,\ w\,)$$
  has exponential growth.

Is $w \in \{y_{2^{2\,\ell+1}}\ :\ \ell \geqslant 2\}$— $\boxed{\text{and, consequently, } \mathcal{J}}$ —Diophantine?

An unproven assertion implying that $w \in \{y_{2^{2\,\ell+1}} : \ell \geqslant 0\}$ is Diophantine

The following are necessary and sufficient conditions in order that

$$w \in \{y_{2^{2\,\ell+1}} \,:\, \ell \geqslant 0\}$$

holds:

An unproven assertion implying that $w \in \{y_{2^{2\ell+1}} : \ell \geqslant 0\}$ is Diophantine

The following are necessary and sufficient conditions in order that

$$w \in \{y_{2^{2\ell+1}} \, : \, \ell \geqslant 0\}$$

holds:

(I) $w > 3$

(II) $11\, w^2 + 1 = \square$

(III) $(\exists\, v\,,\ u)\ w = \ v^2 \pm v\, u + 3\, u^2$

(IV) $(\boldsymbol{r}^2 + \boldsymbol{r}\,\boldsymbol{s} + 3\,\boldsymbol{s}^2)\,(\boldsymbol{v}^2 + \boldsymbol{v}\boldsymbol{u} + 3\,\boldsymbol{u}^2) \nmid w$
for any non-trivial *integer* solution to
$$11\ \left(r^2 + r\, s + 3\, s^2\right)^2 - \left(\upsilon^2 + \upsilon\, u + 3\, u^2\right)^2 \ \ = \ \ 2$$

An unproven assertion implying that $w \in \{y_{2^{2\ell+1}} : \ell \geqslant 0\}$ is Diophantine

The following are necessary and sufficient conditions in order that

$$w \in \{y_{2^{2\ell+1}} : \ell \geqslant 0\}$$

holds:

(I) $w > 3$

(II) $11\,w^2 + 1 = \Box$

(III) $(\exists\, v\,,\ u)\ w = v^2 \pm v\,u + 3\,u^2$

(IV) $(\boldsymbol{r}^2 + \boldsymbol{r}\,\boldsymbol{s} + 3\,\boldsymbol{s}^2)\,(\boldsymbol{v}^2 + \boldsymbol{v}\boldsymbol{u} + 3\,\boldsymbol{u}^2) \nmid w$

for any non-trivial *integer* solution to

$$11\,\left(r^2 + r\,s + 3\,s^2\right)^2 - \left(\upsilon^2 + \upsilon\,u + 3\,u^2\right)^2 = 2$$

☺ ☺ ☺

This results in a Diophantine specification $\boxed{\text{if}}$ "*the number of solutions to this novel quaternary quartic is finite*" !

An unproven assertion implying that $w \in \{y_{2^{2\ell+1}} : \ell \geqslant 0\}$ is Diophantine

The following are necessary and sufficient conditions in order that

$$w \in \{y_{2^{2\ell+1}} : \ell \geqslant 0\}$$

holds:

(I) $w > 3$

(II) $11\, w^2 + 1 = \square$

(III) $(\exists\, v\,,\ u)\ w = v^2 \pm v\, u + 3\, u^2$

(IV) $(\boldsymbol{r}^2 + \boldsymbol{r}\,\boldsymbol{s} + 3\,\boldsymbol{s}^2)\,(\boldsymbol{v}^2 + \boldsymbol{v}\boldsymbol{u} + 3\,\boldsymbol{u}^2) \nmid w$ for any non-trivial *integer* solution to

$$11\ \left(r^2 + r\,s + 3\,s^2\right)^2 - \left(\upsilon^2 + \upsilon\,u + 3\,u^2\right)^2 \ = \ 2$$

:-) :-) :-)

The only potential source of multiple-solutions here is condition (III), which, anyhow, is finite-fold

The issue as whether

$$11\ \left(r^2 \pm r\,s + 3\,s^2\right)^2 - \left(v^2 \pm v\,u + 3\,u^2\right)^2 \;=\; 2$$

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

$$\begin{cases} 11\,\xi^2 - \eta^2 & = \; 2 \\ \xi\,\eta & = \; \nu^2 + \nu\,t + 3\,t^2 \end{cases}$$

over $\mathbb{Z}$.

The issue as whether

$$11\ \left(r^2 \pm r\,s + 3\,s^2\right)^2 - \left(v^2 \pm v\,u + 3\,u^2\right)^2 \;=\; 2$$

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

$$\begin{cases} 11\,\xi^2 - \eta^2 & = \; 2 \\ \xi\,\eta & = \; \nu^2 + \nu\,t + 3\,t^2 \end{cases}$$

over $\mathbb{Z}$.

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.

Thanks for your attention! (References ☞)

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

Martin Davis.
Lecture Notes in Logic.
Courant Institute of Mathematical Sciences, New York University, 1993.

Martin Davis, Yuri Matijasevič, and Julia Robinson.
Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution.
In *Mathematical Developments Arising From Hilbert Problems*, volume 28 of *Proceedings of Symposia in Pure Mathematics*, pages 323–378, Providence, RI, 1976. American Mathematical Society.
Reprinted in [Rob96, p. 269ff.].

Martin Davis, Hilary Putnam, and Julia Robinson.
The decision problem for exponential Diophantine equations.
Annals of Mathematics, Second Series, 74(3):425–436, 1961.

J. P. Jones and Y. V. Matijasevič.
Register machine proof of the theorem on exponential Diophantine representation of enumerable sets.
The Journal of Symbolic Logic, 49(3):818–829, 1984.

Ju. V. Matijasevič.
Enumerable sets are Diophantine.
Soviet Mathematics. Doklady, 11(3):354–358, 1970.
(Translated from [Mat70b]).

Yu. V. Matiyasevich.
Diofantovost' perechislimykh mnozhestv.
Doklady Akademii Nauk SSSR, 191(2):279–282, 1970.
(Russian. Available in English translation as [Mat70a]; translation reprinted in [Sac03, pp. 269–273]).

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 Yu. V. Matiyasevich, Existence of noneffectivizable estimates in the theory of exponential Diophantine equations, *Journal of Soviet Mathematics*, 8(3):299–311, 1977).

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

Yuri Matijasevič and Julia Robinson.
Reduction of an arbitrary diophantine equation to one in 13 unknowns.
Acta Arithmetica, XXVII:521–553, 1975.
Reprinted in [Rob96, p. 235ff.].

Julia Robinson.
Existential definability in arithmetic.
Transactions of the American Mathematical Society, 72(3):437–449, 1952.
Reprinted in [Rob96, p. 47ff.].

Julia 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.

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

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