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

MEMORANDUM
RM-5494-PR
FEBRUARY 1968

ONE EQUATION TO RULE THEM ALL

Martin Davis

This research is supported by the United States Air Force under Project RAND — Contract No. F44620-67-C-0045 — monitored by the Directorate of Operational Requirements and Development Plans, Deputy Chief of Staff, Research and Development, Hq USAF. RAND Memoranda are subject to critical review procedures at the research department and corporate levels. Views and conclusions expressed herein are nevertheless the primary responsibility of the author, and should not be interpreted as representing the official opinion or policy of the United States Air Force or of The RAND Corporation.

The RAND Corporation
1700 MAIN ST. • SANTA MONICA • CALIFORNIA • 90406

Published by The RAND Corporation

PREFACE

Some of the most significant applications of recursive function theory have been those made to decision problems arising in other areas of mathematics. For example, Novikoff and Boone demonstrated independently that the word problem for groups is recursively unsolvable. Since about 1950, continuing attempts have been made to prove that Hilbert's tenth problem is unsolvable, that is, that no algorithm exists for determining whether an arbitrary polynomial with integer coefficients has a root in integers. In this Memorandum, which is the result of such an attempt, it is shown that if a certain single diophantine equation has no non-trivial solutions, then Hilbert's tenth problem is unsolvable.

The author wishes to acknowledge helpful discussions with Robert DiPaola, Oliver Gross, Hilary Putnam, Norman Shapiro, and Joel Spencer. The ideas of Section 3 are from unpublished joint work with Hilary Putnam done during the summer of 1962.†

Professor Martin Davis, a consultant, is on the faculty of New York University.

---

†This material is referred to as "Proposition 2" in [4]. As stated, the "proposition" requires the following correction: Replace "$r^2 + ds^2$" by "$a_1 a_1'(r^2 + ds^2)$."

SUMMARY

It is shown that if a particular exhibited diophantine equation has no non-trivial solutions, then Hilbert's tenth problem is recursively unsolvable.

Let H stand for the assertion:

The equation

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

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

The truth of H must be left open; however, in this study it is proved that

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, the methods used in this study yield a result considerably stronger than the statement above. These methods can be readily adapted to obtain various other hypotheses about which demonstrations can be made similar to that for H. The Memorandum concludes with a report on numerical calculations (some using the JOSS‡ system) made in a search for counterexamples to H.

†See Chapter 7 of [1], [3], [4], [5], and [6].

‡JOSS is the trademark and service mark of The RAND Corporation for its computer program and services using that program.

CONTENTS

ONE EQUATION TO RULE THEM ALL

1. INTRODUCTION[†]

At the International Congress of Mathematicians held at Paris in 1900, David Hilbert [8] posed a series of problems that were to stand as a challenge to future generations of mathematicians, and that have had a profound effect on the subsequent history of mathematics. The tenth problem of this series, which has come to be known as "Hilbert's tenth problem," is one of several remaining Hilbert problems that have resisted the intense efforts of mathematicians everywhere. It reads:

> 10. Entscheidung der Lösbarkeit einer diophantischen Gleichung.
> Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoeffiziensten sei vorgelegt; man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.[‡]

Given the failure of mathematicians to develop a general theory of diophantine equations, the modern theory of recursive functions suggests a "solution" to Hilbert's tenth problem which is radically different from any that could have been envisaged in 1900, namely, that the problem of finding such an algorithm is in a fundamental sense

---

[†] The Introduction was prepared by members of The RAND Corporation staff.

[‡] 10. Determining the solvability of a diophantine equation.
Let a diophantine equation with an arbitrary number of unknowns and with integer coefficients be given; a procedure is desired such that by means of a finite number of operations it can be decided whether the equation has a solution in integers.

unsolvable[†]: i.e., there is no such algorithm as is desired. This Memorandum proves that if a certain specific diophantine equation has no non-trivial integral solutions, then Hilbert's tenth problem is unsolvable in the above sense.

To place this Memorandum in context, a brief review of the previous work done toward establishing the unsolvability of the problem is in order. Post [10] was the first to formulate Hilbert's tenth problem as a decision problem of a recursively enumerable set. The author [2] proved that every recursively enumerable relation can be represented in the form

$$\bigvee_{y} \bigwedge_{k=0}^{y} D(x_1, x_2, \ldots, x_n, k, y) ,$$

where D is a diophantine predicate, that is, a polynomial equation prefixed by a block of existential quantifiers. Hence there are recursively unsolvable problems of this form, and if it were known that the class of diophantine predicates is closed under bounded universal quantification, a proof would follow that Hilbert's tenth problem is unsolvable.

In a paper which has remained basic to later research, Julia Robinson [11] investigated the relation between diophantine predicates and predicates of (roughly speaking) exponential order of growth. This paper suggested the consideration of the decision problem for exponential diophantine equations, that is, for those diophantine equations in which the exponents appearing in polynomials are treated as variables. Research on this problem culminated in [3], where it was shown that all

---

[†]It is interesting that Hilbert emphasized the possibility that, as with the famous construction problems of Greek mathematics, the solution to a problem is in terms which could not have been imagined by the proposer of the problem.

recursively enumerable sets are exponential diophantine, and that therefore the decision problem for exponential diophantine equations is--in a sense precise to recursive function theorists--of the highest degree of unsolvability for decision problems about recursively enumerable sets.

There also stemmed from [11] the following hypothesis, which has come to be known as J.R.: There is a diophantine predicate of exponential order of growth, in the sense of [11]. It follows from [5] that J.R. implies that all recursively enumerable sets are diophantine and hence that Hilbert's tenth problem is unsolvable. Most of the recent work on the problem has been devoted to establishing J.R. This Memorandum falls into this category, since it proves that if a particular diophantine equation has no non-trivial solutions, then J.R. holds.

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

Below, p is always 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 [9], we have

$$x_n + y_n\sqrt{7} = (x_1 + y_1\sqrt{7})^n .$$

Moreover, we may calculate x_1, y_1 from the fact that y_1 is the least y for which $1 + 7y^2$ is a square and $x_1 = \sqrt{1 + 7y_1^2}$. This gives $x_1 = 8$, $y_1 = 3$.

Lemma 2. $(x_n, y_n) = 1$.

Proof. $d \mid x_n$ and $d \mid y_n$ implies $d \mid (x_n^2 - 7y_n^2)$, i.e., $d \mid 1$.

Lemma 3. *The sequences x_n, y_n are both solutions of the second-order difference equation*

$$U_{n+2} = 16U_{n+1} - U_n .$$

Proof. Let $\theta = 8 + 3\sqrt{7}$, $\theta' = 8 - 3\sqrt{7}$. Then, $\theta + \theta' = 16$, $\theta\theta' = 1$, so that $\theta^2 - 16\theta + 1 = 0$. Hence $\theta^{n+2} - 16\theta^{n+1} + \theta^n = 0$. That is,

$$x_{n+2} + y_{n+2} \sqrt{7} = 16(x_{n+1} + y_{n+1} \sqrt{7}) - (x_n + y_n \sqrt{7}) .$$

Lemma 4. *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 implies that $x_{n+2} \equiv x_n \pmod 2$, $y_{n+2} \equiv y_n \pmod 2$.

Lemma 5. $x_{2n} = (x_n)^2 + 7(y_n)^2$, $y_{2n} = 2x_n y_n$.

Proof.

$$x_{2n} + y_{2n} \sqrt{7} = (x_n + y_n \sqrt{7})^2 = (x_n^2 + 7y_n^2) + 2x_n y_n \sqrt{7} .$$

Lemma 6. *Let $n = 2^m \cdot k$, $m > 0$. Then,*

$$y_n = 2^m x_k y_k \prod_{0<i<m} x_{2^i \cdot k} .$$

Proof. For $m = 1$, the result is given by Lemma 5. Proceeding by induction (and using Lemma 5),

$$y_{2^{m+1}\cdot k} = 2x_{2^m\cdot k}\, y_{2^m\cdot k} = 2^{m+1}\, x_k y_k \prod_{0<i<m} x_{2^i\cdot k} .$$

Lemma 7.

$$y_{2^m} = 2^{m+3}\cdot 3 \prod_{0<i<m} x_{2^i} .$$

Proof. Take $k = 1$ in Lemma 6.

Lemma 8. $3 \mid y_n$.

Proof. This is true for $n = 0, 1$, and hence by Lemma 3 must be true for all n.

Lemma 9. $y_{2k+1} = (3x_k + 7y_k)(x_k + 3y_k)$.

Proof.

$$x_{2k+1} + y_{2k+1}\sqrt{7} = (x_k + y_k\sqrt{7})^2(8 + 3\sqrt{7})$$

$$= ((x_k^2 + 7y_k^2) + 2x_k y_k\sqrt{7})(8 + 3\sqrt{7}) .$$

Hence,

$$y_{2k+1} = 3x_k^2 + 16x_k y_k + 21y_k^2$$

$$= (3x_k + 7y_k)(x_k + 3y_k) .$$

Lemma 10. $(3x_k + 7y_k,\ x_k + 3y_k) = 1$.

Proof. If $p \mid 3x_k + 7y_k$, $p \mid x_k + 3y_k$, then since $3(x_k + 3y_k) - (3x_k + 7y_k) = 2y_k$, either $p = 2$ or $p \mid y_k$. But by Lemma 4, x_k and y_k have opposite parity, so $p \neq 2$. Hence $p \mid y_k$, and therefore $p \mid [(x_k + 3y_k) - 3y_k]$, i.e., $p \mid x_k$, which contradicts Lemma 2.

3. REPRESENTABLE NUMBERS

A positive integer x will be called *representable* if there are non-negative integers u, v, such that $x = u^2 + 7v^2$. As is well known, the product of representable numbers is representable. (Namely, if $x = \alpha\,\overline{\alpha}$, $y = \beta\,\overline{\beta}$, $\alpha = u + v\sqrt{-7}$, $\beta = r + s\sqrt{-7}$, then $xy = (\alpha\beta)\cdot(\overline{\alpha\beta})$.)

Lemma 11. *2^m is representable if $m \geq 2$.*

Proof. For $m = 2k$, $k \geq 0$, we have $2^{2k} = (2^k)^2 + 7\cdot(0)^2$. If m is odd, $m \geq 2$, then $m = 2k + 3$, $k \geq 0$. Hence $2^m = 2^{2k}\cdot 8$, which is the product of representable numbers since $8 = (1)^2 + 7\cdot(1)^2$.

We shall call an *odd* prime p *poison* if $p \equiv 3$, 5, or 6 (mod 7) and *non-poison* if $p \equiv 1$, 2, or 4 (mod 7).[†] Note that every odd prime $p \neq 7$ is either poison or non-poison, but that 2 is neither.

The following two lemmas are immediate consequences of exercises 9 and 10 on page 81 of [7].

Lemma 12. *If there is a poison prime dividing x to an odd power, then x is not representable.*

Lemma 13. *If x is odd and is not representable, then there is a poison prime which divides x to an odd power.*

We thus find, recalling Lemma 8,

Lemma 14. *For all m, $y_{2^m}/3$ is representable.*

Proof. By Lemma 5, x_{2^i}, $0 < i < m$ is representable for each i. By Lemma 11, 2^{m+3} is representable. The result follows at once from Lemma 7.

Lemma 15. *If $n = 2^m\cdot k$, k, $m > 0$, k is odd and $y_n/3$ is representable, then $y_k/3$ is representable.*

Proof. Suppose $y_k/3$ were not representable. By Lemmas 4 and 13

[†] Of course the "non-poison" primes are just the odd primes which are quadratic residues mod 7.

there is a poison prime p which divides $y_k/3$ to an odd power. Since by Lemma 5 each $x_{2^i \cdot k}$, $0 < i < m$ is representable, Lemma 12 implies that p divides each of these numbers to an even (perhaps 0) power. Moreover $p \nmid 2^m$ and, by Lemma 2, $p \nmid x_k$. So, by Lemma 6, p divides $y_n/3$ to an odd power, which by Lemma 12 contradicts the hypothesis.

Lemma 16. *If $y_{2k+1}/3$ is representable, so are $x_k + 7(y_k/3)$ and $x_k + 3y_k$.*

Proof. The result follows at once from Lemmas 8, 9, 10, 13, and 14.

Finally, we obtain:

Theorem 1. *If for some $n > 0$ not a power of 2, $y_n/3$ is representable, then the system of diophantine equations*

$$X^2 - 63Y^2 = 1 \ ,$$

$$X + 7Y = u^2 + 7v^2 \ ,$$

$$X + 9Y = r^2 + 7s^2$$

has a non-negative integer solution for which $Y \neq 0$.

Proof. By Lemmas 15 and 16, the hypothesis implies there are representable numbers $x_k + 7(y_k/3)$, $x_k + 3y_k$, $k > 0$. Setting $X = x_k$, $Y = y_k/3$, we have numbers u, v, r, s with

$$X + 7Y = u^2 + 7v^2 \ ,$$

$$X + 9Y = r^2 + 7s^2 \ .$$

Moreover,

$$X^2 - 63Y^2 = x_k^2 - 63(y_k/3)^2$$
$$= x_k^2 - 7y_k^2$$
$$= 1 \ .$$

Corollary. *If for some $n > 0$ not a power of 2, $y_n/3$ is representable, then our equation* (*) *has a non-trivial solution.*

Proof. Let X, Y be as in Theorem 1. Then,[†]

$$9(u^2 + 7v^2)^2 - 7(r^2 + 7s^2)^2$$
$$= 9(X^2 + 14XY + 49Y^2) - 7(X^2 + 18XY + 81Y^2)$$
$$= 2(X^2 - 63Y^2)$$
$$= 2 \ .$$

Combining the Corollary with Lemma 14, we obtain:

Theorem 2. *H implies that $y_n/3$ is representable for $n > 0$ if and only if n is a power of 2.*

Corollary. *H implies that $\{y_{2^m}\}$ is a diophantine set.*[‡]

Proof. By the Theorem:

$$y \in \{y_{2^m}\} \longleftrightarrow (\exists\, u,\ v,\ x)[x^2 - 7y^2 = 1 \ \&\ y = 3(u^2 + 7v^2)] \ .$$

4. A DIOPHANTINE SET OF EXPONENTIAL GROWTH

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

[†] This simple calculation was suggested by Oliver Gross.

[‡] See Chapter 7 of [1].

Lemma 17. $y_{n+1} = 3x_n + 8y_n$.

Proof. $x_{n+1} + y_{n+1}\sqrt{7} = (x_n + y_n\sqrt{7})(8 + 3\sqrt{7})$, which gives the result.

Lemma 18. For $n \geq 1$, $8y_n < y_{n+1} < 16y_n$.

Proof. Use Lemmas 3 and 17.

Lemma 19. For $n \geq 1$, $3 \cdot 8^{n-1} \leq y_n \leq 3 \cdot 16^{n-1}$.

Proof. Follows by induction from Lemma 18.

We shall write $GPT(m)$ for the largest power of 2 which divides m; e.g., $GPT(5) = 1$, $GPT(12) = 4$.

Lemma 20. *$a \geq GPT(b)$ is a diophantine predicate.*

Proof.

$$a \geq GPT(b) \leftrightarrow (\exists\, x, y)[b = y(2x + 1)\ \&\ a \geq y] .$$

In what follows we write

$$\rho(m, n) \leftrightarrow (\exists\, x)[n \geq 2^x\ \&\ n > 16\ \&\ m = y_{2^x}] .$$

Lemma 21. *For each $k > 0$, there are m, n such that $\rho(m, n)$ and $m > n^k$.*

Proof. Given $k > 0$, choose N such that $r > N$ implies $8^{r-1} > r^k$. Let n be any power of 2 greater than both N and 16 and let $m = y_n$. Then, $\rho(n, m)$ is true, and

$$\begin{aligned} m &= y_n \\ &\geq 3 \cdot 8^{n-1} \\ &> n^k . \end{aligned}$$

Lemma 22. *$\rho(m, n)$ implies $m < n^n$.*

Proof. $\rho(m, n)$ implies

$$\begin{aligned} m &= y_{2^x} \\ &\le y_n \\ &\le 3 \cdot 16^{n-1} \\ &< n^n , \end{aligned}$$

since $n > 16$.

Finally, we note the relationship:

Lemma 23.

$$\rho(m, n) \longleftrightarrow m \in \{y_{2^x}\} \ \& \ n/8 \ge GPT(m) \ \& \ n > 16 .$$

Proof. By Lemmas 4 and 7, $GPT(y_{2^x}) = 2^{x+3}$.

Theorem 3. *H implies that there is a diophantine predicate* $\rho(m, n)$ *such that*

1. *For each* $k > 0$, *there are* m, n *such that* $\rho(m, n)$ *and* $m > n^k$;
2. $\rho(m, n)$ *implies* $m < n^n$.

Proof. This follows at once from the Corollary to Theorem 2, together with Lemmas 21, 22, and 23.

Corollary. *H implies that every recursively enumerable set is diophantine, and therefore that Hilbert's tenth problem is unsolvable.*

Proof. For, our Theorem 3 yields precisely the well-known conditions of Julia Robinson [11].†

5. SOME NUMERICAL CALCULATIONS

Let us first note:

†In particular see [3], p. 430, Corollary 3.

Lemma 24. *H is equivalent to the assertion that $y_{2k+1}/3$ is never representable.*

Proof. Immediate from Theorem 2 and Lemma 15.

The numbers y_{2k+1} grow much too rapidly for direct computation to be feasible. Our procedure was to note that the factors $x_k + 7(y_k/3)$, $x_k + 3y_k$ of $y_{2k+1}/3$ both satisfy the same second-order difference equation ($U_{n+2} = 16 \cdot U_{n+1} - U_n$) already employed. Hence, we used JOSS to generate these factors mod p for various primes p to check for the presence of poison prime factors. Our calculations showed that $y_m/3$ *is not representable for all odd* $m \leq 69$. For $y_{71}/3$, JOSS was used to find the factorization

$$x_{35} + 3y_{35} = 569 \cdot 12497 \cdot 14767 \cdot 12342543109540897423342896942089.$$

No factors were found for

$$x_{35} + 7(y_{35}/3) = 114299078530967137438991431679759903568432 1.^{\dagger}$$

None of the primes 569, 12497, 14767 are poison. However, John Selfridge[‡] has reported a computation on an IBM 7090 at UCLA showing that both of the large remaining factors are *composite*. However, he reports that the smaller of these has no factor $< \frac{1}{3} \cdot 10^9$, and the larger no factor $< 3 \cdot 10^6$.

[†]The decimal representations of the two very large numbers listed were found by Joel Spencer, using JOSS.

[‡]Oral communication.

REFERENCES

1. Davis, Martin, *Computability and Unsolvability*, McGraw-Hill Book Company, Inc., New York, 1958.

2. Davis, Martin, "Arithmetical Problems and Recursively Enumerable Predicates," *The Journal of Symbolic Logic*, Vol. 18 (1953), pp. 33-41.

3. Davis, Martin, Hilary Putnam, and Julia Robinson, "The Decision Problem for Exponential Diophantine Equations," *Ann. of Math.* (2), Vol. 74 (1961), pp. 425-436.

4. Davis, Martin, "Applications of Recursive Function Theory to Number Theory," *Symposium in Prime Math.*, Vol. 5 (1962), pp. 135-138.

5. Davis, Martin, "Extensions and Corollaries of Recent Work on Hilbert's Tenth Problem," *Illinois J. Math.*, Vol. 7 (1963), pp. 246-250.

6. Davis, Martin, and Hilary Putnam, "Diophantine Sets Over Polynomial Rings," *Illinois J. Math.*, Vol. 7 (1963), pp. 251-256.

7. Dickson, Leonard E., *Introduction to the Theory of Numbers*, University of Chicago Press, Chicago, Illinois, 1929. Reprinted by Dover Publications, 1957.

8. Hilbert, David, "Mathematische Probleme," Vortrag, gehalten auf dem internationalen Mathematiker-Kongress zu Paris 1900. *Nachr. K. Wiss. Göttingen, Math. Phys.* Kl. 1900, pp. 253-297. Reprinted in *Arch. Math. Phys.*, 3rd series, 1 (1901), pp. 44-63, 213-237. English translation, *Bull. Amer. Math. Soc.*, Vol. 8, (1901-1902), pp. 437-479.

9. Nagell, Trygve, *Introduction to Number Theory*, John Wiley & Sons, New York, 1951.

10. Post, Emil L., "Recursively Enumerable Sets of Positive Integers and Their Decision Problems," *Bull. Amer. Math. Soc.*, Vol. 50 (1944), pp. 284-316.

11. Robinson, Julia, "Existential Definability in Arithmetic," *Trans. Amer. Math. Soc.*, Vol. 72 (1952), pp. 437-449.