Diophantine Equations & Computation

I. Survey

Martin Davis

Professor Emeritus
Courant Institute, NYU

Visiting Scholar
UC Berkeley

Unless otherwise stated, we'll work with the *natural numbers*:

$$N = \{0, 1, 2, 3, \ldots\}$$

Consider a Diophantine equation

$$D(a_1, a_2, \ldots, a_n, x_1, x_2, \ldots, x_m) = 0$$

Here, $a_1, a_2, \ldots, a_n$ are *parameters*, and , $x_1, x_2, \ldots, x_m$ are *unknowns*. For such a given equation, it is usual to ask:

For which values of the parameters does the equation have a solution in the unknowns? In other words, find:

$$\{< a_1, \ldots, a_n >| \; \exists x_1, \ldots, x_m [D(a_1, \ldots, x_1, \ldots) = 0]\}$$

We think of the equation $D = 0$ as furnishing a *definition* of the corresponding set.

Examples

- The Pell equation $x^2 - d(y+1)^2 = 1$ *defines* the set consisting of 0 and the numbers not perfect squares.
- $(x+1)^n + (y+1)^n = (z+1)^n$ defines the set $\{1, 2\}$.
- $a = (x+2)(y+2)$ defines the set of *composite numbers*.
- $a = (2x+3)(y+1)$ defines the set of numbers not powers of 2.

Considering Diophantine equations

$$F(a_1, a_2, \ldots, a_n, x_1, x_2, \ldots, x_m) = 0$$

as defining the corresponding set

$$\{< a_1, \ldots, a_n >| \exists x_1, \ldots, x_m[F(a_1, \ldots, x_1, \ldots) = 0]\}$$

we distinguish three classes:

- a set is called *Diophantine* if it has such a definition in which F is a polynomial with integer coefficients. We write $\mathcal{D}$ for the *class of Diophantine sets.*
- a set is called *exponential Diophantine* if it has such a definition in which F is an exponential polynomial with integer coefficients. We write $\mathcal{E}$ for the *class of exponential Diophantine sets.*
- a set is called *recursively enumerable* (or *listable*)if it has such a definition in which F is a computable function. We write $\mathcal{R}$ for the *class of recursively enumerable sets.* ("Recursively enumerable" is abbreviated: r.e.)

Evidently:

$$\mathcal{D} \subseteq \mathcal{E} \subseteq \mathcal{R}$$

Converse inclusions?

Remark

The system of equations:

$$\begin{array}{rcl} E_1 & = & 0 \\ E_2 & = & 0 \\ \ldots & \ldots & \\ E_n & = & 0 \end{array}$$

is equivalent to the single equation

$$E_1^2 + E_2^2 + \ldots + E_n^2 = 0$$

So, a system of equations is as good as a single equation for giving a Diophantine definition.

Hilbert's 10th problem: Find an algorithm to determine whether a given polynomial Diophantine equation with integer coefficients has an integer solution.

It's equivalent to the analogous problem for solutions in natural numbers:

- $p(x_1, \ldots, x_n) = 0$ has a solution in integers if and only if at least one of the 2^n equations
$$p(\pm x_1, \ldots, \pm x_n) = 0$$
has a solution in natural numbers.
- $p(x_1, \ldots, x_n) = 0$ has a solution in natural numbers if and only if
$$p(q_1^2 + r_1^2 + s_1^2 + t_1^2, \ldots, q_1^2 + r_1^2 + s_1^2 + t_1^2) = 0$$
has an integer solution.

Theorem (Church,Post,Turing) *There is a set $K \subseteq N$ such that $K \in \mathcal{R}$, but K is not computable, i.e., there is no algorithm for testing membership in K.*

MRDP (=DPRM) Theorem: $\mathcal{D} = \mathcal{R}$.

$$K = \{a \in N \mid \exists x_1, \ldots, x_n[\pi(a, x_1, \ldots, x_n) = 0]\}$$

with π a polynomial. So, there is no algorithm to determine, for given a, whether the corresponding equation has a solution .

Hence, Hilbert's 10th problem is unsolvable.

History of MRDP Theorem

Davis 1950: For every $S \in \mathcal{R}$, there is a polynomial p such that

$$S = \{a \mid \exists y \forall k_{\leq y} \exists x_1, \ldots, x_n [\, p(a, k, y, x_1, \ldots, x_n) = 0]\}$$

Julia Robinson's Hypothesis (JR) 1950: There is a function $f \in \mathcal{D}$ such that $f(x) = O(x^x)$ but $f(x) \neq O(x^k)$ for any positive integer k.

Definition: $\exp = \{< a, b, c >\mid c = a^b\}$.

Robinson 1950: JR $\Rightarrow \exp \in \mathcal{D} \Rightarrow \mathcal{D} = \mathcal{E}$.

Davis, Putnam, Robinson 1961: $\mathcal{E} = \mathcal{R}$. Hence, JR $\Longleftrightarrow \mathcal{D} = \mathcal{R}$

Matiyasevich (1970): $F_{2n} \in \mathcal{D}$ (where F_n is the nth Fibonacci number). **Hence JR.**

The positive numbers a for which

$$p(a, x_1, \ldots, x_n) = 0$$

has a solution is the positive part of the range of the polynomial $a(1-p^2(a, x_1, \ldots, x_n))$. So as Hilary Putnam remarked: *The set of positive integers in an r.e. set is always representable as the positive part of the range of a polynomial.*

Theorem:(Jones,Sato,Wada,Wiens 1976) The positive prime numbers are the positive part of the range of:

$$\begin{aligned}
(k+2)\{1 \;&-\; [wz+h+j-q]^2 \\
&-\; [(gk+2g+k+1)(h+j)+h-z]^2 \\
&-\; [2n+p+q+z-e]^2 \\
&-\; [16(k+1)^3(k+2)(n+1)^2+1-f^2]^2 \\
&-\; [e^3(e+2)(a+1)^2+1-o^2]^2 \\
&-\; [(a^2-1)y^2+1-x^2]^2 \\
&-\; [16r^2y^4(a^2-1)+1-u^2]^2 \\
&-\; [n+\ell+v-y]^2 \\
&-\; \left[\Big((a+u^2(u^2-a))^2-1\Big)(n+4dy)^2+1-(x+cu)^2\right]^2 \\
&-\; [(a^2-1)\ell^2+1-m^2]^2 \\
&-\; [q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2 \\
&-\; [z+p\ell(a-p)+t(2ap-p^2-1)-pm]^2 \\
&-\; [ai+k+1+\ell-i]^2 \\
&-\; [p+\ell(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2\}
\end{aligned}$$

Theorem (Davis 1972) Let $\mathcal{C} = \{0, 1, 2, \ldots, \aleph_0\}$. Let $\mathcal{A} \subseteq \mathcal{C}$ where $\mathcal{A} \neq \emptyset$ and $\mathcal{A} \neq \mathcal{C}$. Then, there is no algorithm to determine of a given polynomial Diophantine equation whether the number of solutions of that equation belongs to $\mathcal{A}$.

Corollary There is no algorithm to determine of a given polynomial Diophantine equation whether the number of solutions of that equation is a prime number, is infinite, is the sum of two squares, etc.

Universal Diophantine Equation

Theorem There is a polynomial Diophantine equation

$$p(a, n, x_1, \ldots, x_m) = 0 \tag{1}$$

such for every r.e. set S of natural numbers, there is an n such that $a \in S$ if and only if (1) has a solution $x_1, \ldots, x_m$.

How small can the degree of p be? By a device of Skolem, 4.

What about m, the number of unknowns? Matiyasevich-Robinson: m can be 13. Even (Matiyasevich) 9.

James Jones has investigated the tradeoff between the degree (δ) and the number of unknowns (ν) in a universal equation.

ν	δ	ν	δ	ν	δ
58	4	28	20	21	96
38	8	26	24	19	2668
32	12	25	28	13	6.6×10^{43}
29	16	24	36	9	1.6×10^{45}

A Π_1 sentence is one that can be expressed in the form

"For all natural numbers x, $R(x)$"

where $R(x)$ is a computable condition.

Corollary. Every Π_1 sentence can be transformed into an equivalent sentence of the form:

$$\forall x_1, x_2, \ldots, x_n \, p(x_1, x_2, \ldots, x_n) \neq 0$$

where p is a polynomial with integer coefficients.

Proof. The set $\{x \mid \neg R(x)\}$ is certainly r.e. Hence it is Diophantine. So we can write: $\forall x R(x)$
$\Leftrightarrow \neg\exists x \neg R(x)$
$\Leftrightarrow \neg\exists x \exists u_1, u_2, \ldots, u_m \, p(x, u_1, u_2, \ldots, u_m) = 0$
$\Leftrightarrow \forall x \forall u_1, u_2, \ldots, u_m \, p(x, u_1, u_2, \ldots, u_m) \neq 0 \quad \square$

Theorem: The Riemann Hypothesis is Π_1.

$$\text{Let } \delta(x) = \prod_{n<x} \prod_{j \leq n} \eta(j)$$

where $\eta(j) = 1$ unless j is a prime power and where $\eta(p^k) = p$. Then (Davis, Matiyasevich, Robinson) the Riemann Hypothesis is equivalent to the statement:

$$\left[\sum_{k \leq \delta(n)} \frac{1}{k} - \frac{n^2}{2}\right]^2 < 36n^3 \text{ for } n = 1, 2, 3, \ldots$$

Gödel Incompleteness

Definition. A *Diophantine proof system* is an algorithm that generates true statements of the form:

$$\forall x_1, \ldots, x_m [p(x_1, \ldots, x_m) \neq 0] \qquad (1)$$

(I.e., this equation has no solutions in N.)

If Γ is a Diophantine proof system, we write

$$\Gamma \vdash \forall x_1, \ldots, x_m [p(x_1, \ldots, x_m) \neq 0],$$

$$\Gamma \not\vdash \forall x_1, \ldots, x_m [p(x_1, \ldots, x_m) \neq 0]$$

to indicate, respectively, that (1) is, or is not, generated by Γ.

Recall:

$$K = \{a \in N \mid \exists x_1, \ldots, x_n [\pi(a, x_1, \ldots, x_n) = 0]\}$$

Incompleteness Theorem. For every Diophantine proof system Γ, there is a number a_0 such that

- $\pi(a_0, x_1, \ldots, x_n) = 0$ has no solutions.
- $\Gamma \not\vdash \forall x_1, \ldots, x_m [\pi(a_0, x_1, \ldots, x_n) \neq 0]$

Otherwise, an algorithm to test a given a_0 for membership in K would be obtained by simultaneously searching for a solution to the equation, and using Γ to try to show it has no solutions. Depending on which process terminates first, a_0 does or does not belong to K.

Hilbert's 10th Problem can be stated for many rings. One area of research has considered the ring of integers of algebraic extensions of the rational numbers. The following result was obtained by applying class field theory to theorems of Denef and Lipschitz, the pioneers in this area:

Theorem: (Shlapentokh-Shapiro) *Hilbert's 10th Problem is unsolvable over the ring of integers of any algebraic extension of the rationals with an Abelian Galois group.*

Also open, and apparently very difficult, is Hilbert's 10th Problem over the rationals. In this connection, Bjorn Poonen has obtained a very interesting result making use of elliptic curves: As usual let $\pi(x)$ stand for the number of prime numbers $\leq x$. If S is a set of primes, let $\pi_S(x)$ be the number of elements of S that are $\leq x$.

Theorem: (Poonen 2003) *There is a computable set S of prime numbers such that*

$$\lim_{x \to \infty} \frac{\pi_S(x)}{\pi(x)} = 1$$

and Hilbert's 10th problem is unsolvable over the ring of all rational numbers whose denominators are divisible by a prime in S.

HOLD THE PRESSES!

Barry Mazur and Karl Rubin recently posted a preprint to the ArXiv that may be of interest to FOM readers. They show that if the Shafarevich-Tate group of an elliptic curve over a number field is always finite (actually they assume something weaker than this), then Hilbert's Tenth Problem has a negative answer over the ring of integers of any number field.

http://arxiv.org/abs/0904.3709

(They acknowledge Poonen and Shlapentokh)