Solving equations in algebra and in arithmetic

Yiannis N. Moschovakis
UCLA and University of Athens

Carnegie Mellon Summer School, 26 June, 2008

Outline

We will consider equations

$$p(x_1, \ldots, x_d) = 0 \qquad (*)$$

where $p(x_1, \ldots, x_d)$ is a polynomial with integer coefficients in d variables and of degree n, e.g.,

$$\begin{aligned} p(x) &= x^6 - x^5 - 3x^2 + 2x + 1 \qquad (d = 1, n = 6) \\ p(x_1, x_2, x_3) &= x_1^5 x_2 - x_2 x_3 + 23 x_1 x_3^{16} - 7 \quad (d = 3, n = 17) \end{aligned}$$

(1) Algebra: Are there real solutions of (*)—and which?
$\mathbb{R}$ = the complete ordered field, $0, -3, \frac{2}{3}, \sqrt{5}, \pi, \ldots \in \mathbb{R}$

(2) Arithmetic: Are there integer solutions of (*)—and which?
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

- Logic: Which is the more difficult problem?

Alebraic equations in one unknown ($d = 1$)

Equation	It has solutions in $\mathbb{R}$ if	The solutions are
$ax + b = 0$	$a \neq 0$	$x = -\frac{b}{a}$
$(2x + 3 = 0)$	(Yes)	$(x = -\frac{3}{2})$
$ax^2 + bx + c = 0$	$b^2 - 4ac \geq 0$	$x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$
$(x^2 + 3x + 1 = 0)$	$(3^2 - 4 = 5 \geq 0, \quad \text{Yes})$	$(x = \frac{-3 \pm \sqrt{5}}{2})$
$p(x) = 0$	Algorithm of Sturm (1803-1855)	approximation algorithms
$(x^6 - x^5$	4 solutions	$1, \approx 1,38879$
$- 3x^2 + 2x + 1 = 0)$		$\approx -0,334734, -1,21465$

Polynomial (long) division

Theorem

For any two polynomials with rational coefficients $f(x), g(x)$*, if* $g(x) \not\equiv 0$ *and* $\deg(f(x)) \geq \deg(g(x))$*, then there exists unique polys* $q(x), r(x)$ *such that*

$$\boxed{f(x) = g(x)q(x) + r(x) \text{ where } r(x) \equiv 0 \text{ or } \deg(r(x)) < \deg(g(x))}$$

With $r^*(x) = -r(x)$, the division equation takes the form

$$\boxed{f(x) = g(x)q(x) - r^*(x)}$$

where again $r^*(x) \equiv 0$ or $\deg(r^*(x)) < \deg(g(x))$

Sturm's algorithm for a real polynomial $p(x)$

- The Sturm sequence of $p(x)$:

$$\begin{aligned}
\boxed{p_0(x)} &= p(x), \quad \boxed{p_1(x)} = p'(x) \quad \text{(the derivative of } p(x)\text{)} \\
p_0(x) &= p_1(x)q_1(x) - \boxed{p_2(x)} \\
p_1(x) &= p_2(x)q_2(x) - \boxed{p_3(x)} \\
&\vdots \\
p_r(x) &= p_{r+1}(x)q_{r+1}(x)
\end{aligned}$$

- $w(\alpha)$ = the number of sign changes in the sequence $(p_0(\alpha), p_1(\alpha), p_2(\alpha), \ldots, p_{r+1}(\alpha))$ (for any real α)

If $p(a)p(b) \neq 0$, then $p(x)$ has $w(a) - w(b)$ roots in the interval (a, b)

An example – thanks to Keith Matthews, http://www.numbertheory.org/php/sturm.html

$$
\begin{aligned}
p_0(x) &= x^6 - x^5 - 3x^2 + 2x + 1 \\
p_1(x) &= 6x^5 - 5x^4 - 6x + 2 \\
p_2(x) &= 5x^4 + 72x^2 - 54x - 38 \\
p_3(x) &= 12x^3 - 19x^2 + 2x + 5 \\
p_4(x) &= -12053x^2 + 8266^x + 5947 \\
p_5(x) &= -107846^x + 63383 \\
p_6(x) &= -77249443861323
\end{aligned}
$$

$$
\begin{aligned}
w(-2) &= \#(81, -258, 438, -171, -58797, 279075, -77249443861323) = 5 \\
w(2) &= \#(25, 102, 222, 29, -25733, -152309, -77249443861323) = 1
\end{aligned}
$$

$$\text{number of roots in } (-2, 2) = 5 - 1 = 4$$

- The coefficients have been multiplied by some K
- These are all the real roots of this polynomial

Tarski's algorithm

Theorem (Tarski, 1930)

There is an algorithm which decides whether an arbitrary elementary (first-order) sentence of algebra is true or false

Examples of elementary sentences of algebra:

- The equation $p(x) = 0$ has 5 (real) solutions
- For all $\vec{x} = (x_1, x_2, \ldots, x_n)[p(\vec{x}) = 0$ or $q(\vec{x}) > 0]$
- There exist real numbers $\vec{x} = (x_1, x_2, \ldots, x_n)$ such that

$$p(\vec{x}) = 0 \text{ and } q_1(\vec{x}) \geq 0 \ldots \text{ and } \ldots q_l(\vec{x}) \geq 0$$

where $p(\vec{x}) = p(x_1, \ldots, x_n), q_1(\vec{x}), \ldots, q_l(\vec{x})$ are polynomials

The elementary (first-order) sentences of algebra

are the syntactically correct words (finite sequences)
from the alphabet of 16 symbols

$0 \quad 1 \quad + \quad - \quad \cdot \quad = \quad <$ (field operations)

$\neg$ (not) $\quad$ & (and) $\quad \vee$ (or) (sentential operators)

$\exists$ (there exists) $\quad \forall$ (for every) (quantifiers)

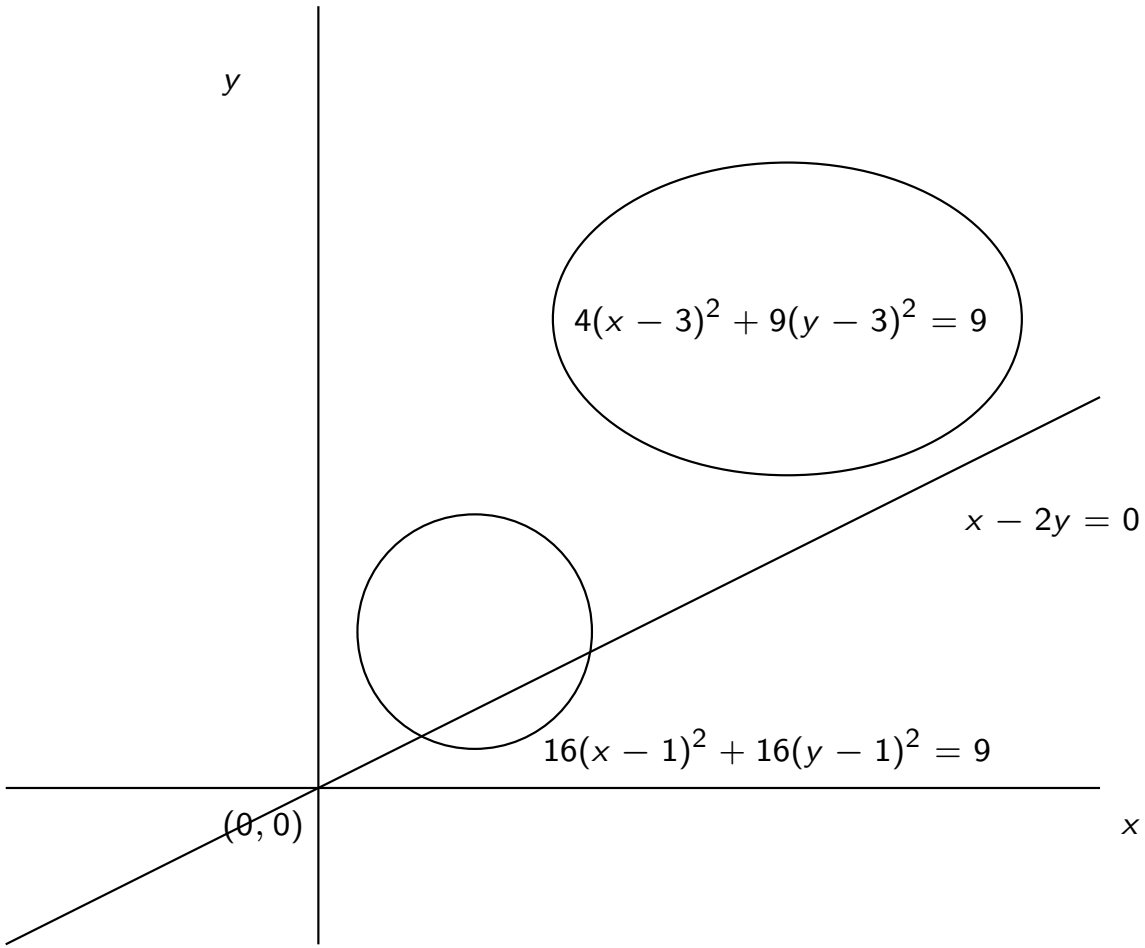
$(\quad)$ (punctuation)

$x \quad |$ (variables $x| \quad x|| \quad x||| \quad \ldots$)

- For every number, there is a bigger one (English)
- $(\forall x)(\exists y)[x < y]$ ("math-English")
- $(\forall x|)(\exists x||)(x| < x||)$ (formal elementary sentence)

- the variables are interpreted by real numbers, in $\mathbb{R}$

Analytic geometry



Euclidean geometry

By using Cartesian coordinates, the problems of Euclidean geometry are translated into algebra problems, many of which can be further translated into elementary sentences, hence:

Corollary (Tarski, 1930)

Elementary Euclidean geometry is decidable,

—i.e., *there is an algorithm which decides whether an arbitrary (elementary) proposition of Euclidean geometry is true or false*

- The circle of Apollonius
- The 3-point line and the 9-point circle of Euler
- ...
- *There are also very substantial applications to computer graphics*

Geometry: intuitively simple sentences are not always elementary

- Elementary: Every angle can be trisected

Not elementary: Every angle can be trisected using ruler and compass

- Elementary: Every cube can be doubled

Not elementary: Every cube can be doubled using ruler and compass

-

Not elementary: The circle of radius 1 can be squared

(Because π is not an algebraic number)

The elementary (first-order) sentences of geometry are (by definition) those which can be expressed in the first-order language of algebra by the use of coordinates

The elementary (first-order) sentences of arithmetic

are *exactly the same as for algebra*. i.e., the syntactically correct words (finite sequences) from the alphabet of 16 symbols

$0 \quad 1 \quad + \quad - \quad \cdot \quad = \quad <$ (field operations)

$\neg$ (not) $\quad$ & (and) $\quad \vee$ (or) (sentential operators)

$\exists$ (there exists) $\quad \forall$ (for every) (quantifiers)

$(\quad)$ (punctuation)

$x \quad |$ (variables$x| \quad x|| \quad x||| \quad \ldots$)

- For every number, there is a bigger one (English)
- $(\forall x)(\exists y)[x < y]$ ("math-English")
- $(\forall x|)(\exists x||)(x| < x||)$ (formal elementary sentence)

- **But**: the variables are interpreted by integers, in $\mathbb{Z}$

Algebra and arithmetic

- "$2x + 3 = 0$ has a solution"

  True in algebra ($x = -\frac{3}{2}$)

  False in arithmetic

- "$x^4 + 2x^3 + x^2 + 5x + 6 = 0$ has a solution"

  2 solutions in algebra (by Sturm, or more simply)

  The integer solutions must divide 6, so we try
  $0, \pm 1, \pm 2, \pm 3, \pm 6$
  and verify that the only integer solution is $x = -2$

Arithmetic is more difficult than algebra!

Theorem (Andrew Wiles, 1994)

The equation $x^n + y^n = z^n$ has no integer solutions when $n > 2$

This was conjectured in 1640 by Fermat, who believed he had proved it, (only the proof "did not fit" in the margin of his notebook!) and so it is known as Fermat's Last Theorem, but no correct proof was known before Wiles' in 1994

Prime numbers

A number $x > 1$ is prime if it is divisible only by 1 and x

Primes: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$

- There are 1229 prime numbers < 10000
- There are infinitely many prime numbers (Euclid)

A number $x > 1$ is a twin prime if both x and $x + 2$ are primes

Twin primes: $3, 5, 11, 17, 29, 41, 59, 71, 101, 107, \ldots$

- There are 205 twin primes < 10000
- Are there infinitely many twin primes?
  Open problem (famously and apparently hopelessly for now)

Arithmetical truths

Theorem (Turing, Church, 1936)

There is no algorithm which decides for an arbitrary sentence of arithmetic whether it is true or false, in other words,

The problem of arithmetical truth is undecidable

Theorem (Matiyasevich 1970, $\Leftarrow$ Davis, Putnam, Robinson)

There is no algorithm which decides for an arbitrary polynomial $p(x_1, \ldots, x_n)$ with integer coefficients whether the equation

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

has integer roots, in other words,

Hilbert's 10th problem is unsolvable

Hilbert 1900: 23 problems

"*which will occupy the mathematicians of the 20th century*"

How can we prove that a problem is absolutely unsolvable?

Church-Turing Thesis (1936)

If a function $f(\alpha)$ on the words from a finite alphabet Σ can be computed by some algorithm, then it can be computed by a program in a computer with an infinitely large hard disk

- The required program can be expressed in any of the usual programming language (Lisp, Pascal, C, Java, . . .)
- "Infinitely large" means "unbounded": the computation of any specific value $f(\alpha)$ will of course be finite

- Rigorous proofs of undecidability are given by a mathematical and logical analysis of the computations which can be done by any computer

- The basic methods for this sort of analysis are due to Kurt Gödel

CT: "The first natural law of mathematics"