Certifying a Number is in A using Polynomials

(This post was done with the help of Max Burkes and Larry Washington.)

During this post, $\mathsf{N}^+\{1,2,3,\ldots\}$.

Recall: Hilbert's 10th problem was to (in todays terms) find an algorithm that would, on input a polynomial $p(x_1,\ldots,x_n) \in \mathsf{Z}[x]$, determine if there are integers $a_1,\ldots,a_n$ such that $p(a_1,\ldots,a_n)=0$.

From the combined work of Martin Davis, Yuri Matiyasevich, Hillary Putnam, and Julia Robinson it was shown that there is no such algorithm. I have a survey on the work done since then, see

`https://arxiv.org/abs/2104.07220`.

The following is a corollary of their work:

Main Theorem Let $A \subseteq \mathsf{N}^+$ be an r.e. set. There is a polynomial $p(y_0,y_1,\ldots,y_n) \in \mathsf{Z}[y_0,y_1,\ldots,y_n]$ such that

$$(x \in A) \text{ iff } (\exists a_1,\ldots,a_n \in \mathsf{N})[(p(x,a_1,\ldots,a_n)=0) \wedge (x>0)]\}.$$

Note

1. Actual examples of polynomials p are of the form

$$p_1(y_0,y_1,\ldots,y_n)^2 + p_2(y_0,y_1,\ldots,y_n)^2 + \cdots + p_m(y_0,y_1,\ldots,y_n)^2$$

   as a way of saying that we want $a_1,\ldots,a_n$ such that the following are all true simultaneously:

   $p_1(x,a_1,\ldots,a_n)=0$, $p_2(x,a_1,\ldots,a_n)=0$, …, $p_m(x,a_1,\ldots,a_n)=0$,

2. The condition $x>0$ can be phrased

$$(\exists z_1,z_2,z_3,z_4)[x-1-z_1^2-z_2^2-z_3^2-z_4^2=0].$$

   This phrasing uses that every natural number is the sum of 4 squares.

The Main theorem gives a ways to certify that $x \in A$: Find $a_1,\ldots,a_n \in \mathsf{Z}$ such that $p(x,a_1,\ldots,a_n)=0$.

Can we really find such $a_1,\ldots,a_n$?

A High School student, Max Burkes, working with my math colleague Larry Washington, worked on the problem of finding $a_1, \ldots, a_n$.

Not much is known on this type of problem. We will see why soon. Here is a list of what is known.

1. Jones, Sato, Wada, Wiens (see

   `https://www.cs.umd.edu/~gasarch/BLOGPAPERS/Jonesh10.pdf`)

   obtained a 26-variable polynomial $q(x_1, \ldots, x_{26}) \in \mathsf{Z}[x_1, \ldots, x_{26}]$ such that

   $$x \in \text{PRIMES iff } (\exists a_1, \ldots a_{26} \in \mathsf{N})[(q(a_1, \ldots, a_{26} = x) \wedge (x > 0)].$$

   To obtain a polynomial that fits the main theorem take

   $$p(x, x_1, \ldots, x_{26}, z_1, z_2, z_3, z_4) = (x - q(x_1, \ldots, x_{26}))^2 + (x - z_1^2 + z_2^2 + z_3^2 + z_4^2)^2.$$

   Jones et al. wrote the polynomial q using as variables $a, \ldots, z$ which is cute since thats all of the letters in the English Alphabet. See their paper pointed to above, or see Max's paper here: `https://www.cs.umd.edu/~gasarch/BLOGPAPERS/BurkesMax.pdf`

2. Nachiketa Gupta, in his Masters Thesis, (see

   `https://www.cs.umd.edu/~gasarch/BLOGPAPERS/PrimeThesis.pdf`)

   tried to obtain the the 26 numbers $a_1, \ldots, a_{26}$ such that $q(a_1, \ldots, a_{26}) = 2$ where q is the polynomial that Jones et al. came up with. Nachiketa Gupta found 22 of them. The other 4 are, like the odds of getting a Royal Fizzbin, astronomical. Could todays computers (21 years later) or AI or Quantum or Quantum AI obtain those four numbers? No, the numbers are just to big.

3. There is a 19-variable polynomial p from the Main Theorem for the set

   $$\{(x, y, k) \colon x^k = y\}.$$

See Max's paper here `https://www.cs.umd.edu/~gasarch/BLOGPAPERS/BurkesMax.pdf` Page 2 and 3, equations 1 to 13. The polynomial p is the sum of squares of those equations. So for example $r(x, y, z) = 1$ becomes $(r(x, y, z) - 1)^2$.

Max Burkes found the needed numbers to prove $1^1 = 1$ and $2^2 = 4$. The numbers for the $2^2 = 4$ are quite large, though they can be written down (as he did). His paper is here

`https://www.cs.umd.edu/~gasarch/BLOGPAPERS/BurkesMax.pdf`

Some Random Thoughts:

1. It is good to know some of these values, but we really can't go much further.

2. Open Question: Can we obtain polynomials for primes and other r.e. sets so that the numbers used are not that large. Tangible goals: (1) Get a complete verification-via-polynomials that 2 is prime. (2) The numbers to verify that $2^3 = 8$.

3. In a 1974 book about progress on Hilbert's problems (I reviewed it in this book rev col:

   `https://www.cs.umd.edu/~gasarch/bookrev/44-4.pdf`.

   there is a chapter on Hilbert's 10 problem by Davis-Matiyasevich-Robinson that notes the following. Using the polynomial for primes, there is a constant c such that, for all primes p there is a computation that shows p is prime in $\leq c$ operations. The article did not mention that the operations are on enormous numbers. OPEN: Is there some way to verify a prime with a constant number of operations using numbers that are not quite so enormous.