Undecidability in Number Theory

Andrew Gilroy

June 23, 2008

In the study of number theory the question often arises: does an equation have a solution? This question can address any given equation, but in the true spirit of mathematics, it can address a general situation. In 1900 David Hilbert posed this question in a list of 23 problems raised after a lecture. It is refered to as Hilbert's tenth problem (H10 for short). The question is whether there exists an algoritm which can denote a simple "Yes" or "No" answer as to whether a given multivariable polynomial with integer coefficients has an integer solution to $f(x_1, x_2, ..., x_n) = 0$. Some 70 years later H10 was answered by Yu Matiyasevich with a definitive "no". The answer lies in the fact that there are more polynomials than there are computable sets.

1 Turing Machines

In order to understand what we are discussing when referring to 'computable' sets we must discuss the concept of the Turing machine. A Turing machine is essentially a finite computer program, however the computer is alloted infinite memory and time. Stated simply, a Turing machine is any algorithm which could in theory be run as a computer program, it is not effected by any physical limitations experienced by real computers.

2 Diophantine, Listable, and Computable Sets

Working beyond the concept of a Turing machine we must first bring up several definitions.

Definition: An set of integers A is diophantine if there exists a polynomail $p(t, x) \in Z[t, x_1, ..., x_n]$ such that:

$$A = \{a \in Z : (\exists x \in Z^n) p(a, x) = 0\}$$

This can be rephrased by saying that a set is diophantine if there is a polynomial with the set as coefficients which has a solution when set to equal zero. For example, the natural numbers are a diophantine subset of the integers, because for every element a in the set of natural numbers there are at most four integers whose squares sum to a. That is, for $a \in N$ there are four integers $\{x_1, x_2, x_3, x_4\}$ such that $x_1^2 + x_2^2 + x_3^2 + x_4^2 = a$.

Another example of a diophantine set is the set of non-prime integers because they can be defined by the (diophantine) equation $a = (x+2)(y+2)$.

Definition: A set A which is a subset of Z is *listable* if there exists an algorithm which will print A.

Any set which can be printed by a Turing machine left running forever is listable, time constraints do not apply. For example the set of integers which are the sum of two squares is listable. This can be accomplished by printing $x^2 + y^2$ for $x < 5$ and $y < 5$, then expanding to $x < 10$ and $y < 10$, and continuing in this manner to infinity.

Definition: A set A which is a subset of Z is *computable* if there exists an algorithm with the ability to decide if a given element is a member of A.

3 The Halting Theorem

H10 is thus a question of whether all diophantine sets are computable. From the definitions it is clear that any computable set must also be listable, however the converse is not apparent. In fact the opposite has been shown, there are sets which are listable, but not computable. In 1936 Turing offered a theorem to the so-called "halting problem" which asks whether there is an algorithm that takes a computer program and integer input and denotes a simple "Yes" or "No" for whether the program will halt on input x:

Theorem: The halting problem is undecidable, that is, no Turing machine can solve it.

We won't discuss the proof in this paper, we are more interested in the corollary which accompanies the theorem.

Corollary: There exists a set that is listable, but not countable.

Proof: Let A be the set of numbers 2^p3^x such that program p halts on input x. By the halting problem theorem, A cannot be computable. However, A is listable as one can construct a program that prints it. Ex: loop over $N = 1, 2, ...$ and during iteration N for each $p, x \leq N$, run p on input x for N steps, and print 2^p3^x if the program halts within these N steps.[1]

4 DPRM Theorem

Finally we are ready to introduce the theorem which gives a negative answer to Hilbert's Tenth Question. It was finalized by Yu Matiyasevich in 1970, however it builds upon work by Davis, Putnam, and Robinson. In essence the proof makes use of a computer constructed from diophantine equations. They showed that such a computer can create a polynomial which has an integer solution if and only if the program halts.

Theorem: A subset of the set of integers is listable if and only if it is diophantine.

In their proof they constructed a diophantine set that is not computable, which provides an obvious negative answer to H10, as it asks for an algoritm to compute whether a diophantine set has an integer solution. By Turing's Theorem we know that the diphantine set constructed by Davis, Putnam, Robinson, and Matiyasevich is not computable, and thus no algorithm can say whether there exists an integer solution.

5 Prime-Producing Polynomials

Another interesting result of the DPRM theorem is a prime-producing polynomial. It has been known for centuries that there are polynomials which produce prime numbers. Euler noted that the polynomial $x^2 + x + 41$ will produce only primes for $0 \leq x \leq 39$. Legendre also stated that x^2+x+17 will produce only primes for $0 \leq x \leq 17$. It has been shown, using the DPRM theorem, that there are polynomials which produce, in its range, the prime numbers.

Theorem: There exists a polynomial

$$F(x_1, ...x_n) \in Z[x_1, ...x_n]$$

[1]Poonen, Bjorn, Undecidability in Number Theory, Notices of the AMS March 2008

such that the positive integers in its range (as a function $N^n \to z$) are exactly the prime numbers.[2]

6 Gödel and Undecidability

In his 23 problems, David Hilbert asked yet another important question on the undecidability of one of the bases for mathematics. Hilbert's Second Question asks for proof that the axioms which make up the basis of arithmetic are consistent. This would essentially show that mathematics can be derived from logic, as the geometric axioms had already been shown to be consistent.

In his two incompleteness theorems Gödel proved that this cannot be done and, in his words, "any effectively generated theory capable of expressing elementary arithmetic cannot be both consistent and complete".

Gödel's First Incompleteness Theorem: For any consistent formal, recursively enumerable theory that proves basic arithmetical truths, an arithmetical statement that is true, but not provable in the theory, can be constructed.1 That is, any effectively generated theory capable of expressing elementary arithmetic cannot be both consistent and complete.

Gödel's Second Incompleteness Theorem: For any formal recursively enumerable (i.e. effectively generated) theory T including basic arithmetical truths and also certain truths about formal provability, T includes a statement of its own consistency if and only if T is inconsistent.

These theorems are of great importance to mathematical logic and mathematics in general. The general topic of undecidability in mathematics depends on these results. These theorems essentially say that mathematics is not infallible and that in order to use arithmetic we must first accept several basic axioms.

David Hilbert posed 23 questions in his famous 1900 lecture, of those, two have had a great effect on the topic of undecidability, both in number theory and in mathematics in general. These questions have given us the results that there is no algorithm which will tell us whether any given diophantine equation has a solution, and we must accept a few basic axioms when working with arithmetic. From these results we are able to make conjectures about prime-producing polynomials among other things, many more important results may be lurking behind these important theorems.

[2]Poonen, Bjorn, Undecidability in Number Theory, Notices of the AMS March 2008