In 1970, Matiyasevič found a polynomial Diophantine equation whose $(m-1)$th positive integer solution, for $m \geq 2$ has the form

$$(m, F_{2m}, x_2, \ldots, x_n).$$

By Lemma 21.3, he inferred

Theorem 21.4. (Matiyasevič)
Every recursively enumerable set of positive integers is Diophantine.

It follows by Lemma 21.1 that a set of positive integers is Diophantine if and only if it is recursively enumerable. We saw in Chapter 20 that not every recursively enumerable set of positive integers is recursive, e.g., the set of positive integers which encode the theorems of mathematics. Therefore, in view of Lemma 21.2, there is no algorithm for testing whether any given polynomial equation has a solution in positive integers. We conclude that *Hilbert's tenth problem is unsolvable.*

Matiyasevič's result had curious repercussions on the existence of *prime representing polynomials.* Consider the polynomial

$$f(x) = x^2 - x + 41.$$

For $x = 1, 2, 3, \ldots, 40$, $f(x)$ is a prime number. While this might convince a physicist that, for any positive integer x, $f(x)$ is always prime, $x = 41$ is a counterexample.

On the other hand, consider the polynomial

$$g(x) = -x^2 + 3.$$

The set of all $g(x) \geq 0$ such that x is a positive is a *subset* of the set of prime numbers, albeit a very small subset.

These examples suggest the following questions:

1. Is there a polynomial with integer coefficients all of whose values for positive integer arguments are primes?
2. Is there a polynomial with integer coefficients such that the set of its *positive* values for positive integer arguments is just the set of primes?

The answer to the first question is 'no', as the reader will be invited to verify in the Exercises. Surprisingly, the answer to the second question is 'yes'. This uses nothing about the set of prime numbers except that it is recursively enumerable, hence Diophantine by Theorem 21.4.

Theorem 21.5. (Putnam)
For any Diophantine set A_p there is a polynomial

$$q(t, x_1, x_2, \ldots, x_n)$$

with integer coefficients such that A_p is the set of all positive values of $q(t, x_1, \ldots, x_n)$ for positive integers $t, x_1, \ldots, x_n$.

Proof: We recall that $t \in A_p$ if and only if $p(t, x_1, \ldots, x_n) = 0$. Let

$$q(t, x_1, \ldots, x_n) = t(1 - (p(t, x_1, \ldots, x_n))^2).$$

We shall illustrate the argument by taking $n = 1$.

(a) Suppose t and x are positive integers and $q(t, x) > 0$. Then

$$t(1 - (p(t, x))^2) > 0$$

and hence $1 > (p(t, x))^2$, so $p(t, x) = 0$, and hence $t \in A_p$.

(b) Suppose $t \in A_p$. Then there is a positive integer x such that $p(t, x) = 0$, hence $q(t, x) = t$.

It follows from Putnam's Theorem that there is a polynomial

$$q(t, x_1, \ldots, x_n)$$

with integer coefficients, such that the set of its positive values, for positive integer assignments of the $n + 1$ variables, is exactly the set of prime numbers. Such a polynomial can be found in Browder [1976], p. 331.

Exercises

1. Explain why the set of positive integers which are not powers of 2 is Diophantine.

2. Describe an algorithm for solving Diophantine equations in one variable:
$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$
where the a_i are given integers.

3. Let $f(x)$ be a polynomial with integer coefficients. Show that there is a positive integer x such that $f(x)$ is not prime.

4. Let $f(x_0, x_1, \ldots, x_n)$ be a polynomial with integer coefficients. Show that there are positive integers $x_0, \ldots, x_n$ such that $f(x_0, \ldots, x_n)$ is not prime.

5. Prove that the set $\{2, 3, 4\}$ is Diophantine and find a polynomial $q(t, x_1, \ldots, x_n)$ with integer coefficients whose positive values, for positive integer arguments, are just the members of this set.

6. Find a polynomial with integer coefficients whose positive values, for positive integer arguments, are all and only composite numbers.

22
Lambda Calculus

The Lambda Calculus of Alonzo Church represents an attempt to understand mathematical entities as *functions*. Usually, people think of a function $f : A \to B$ as having a domain A and a codomain B. But, in the *untyped* version of the lambda calculus, one makes the implicit assumption that $A = B$ is some kind of universal set and that f is is defined everywhere; it is even possible to apply f to itself.

We write $f`a$ for the value of $f$ at $a$ and we read this as $f$ *of* $a$. For example, if $f$ is the squaring function, we write $f`a$ for a^2. Similarly, if $\phi(x)$ is the expression $x^3 + x + 1$, we can introduce a function g such that $g`x = \phi(x) \equiv x^3 + x + 1$. It is customary to write $g = \lambda_x(x^3 + x + 1)$, where λ_x is the *abstraction operator.* It is sometimes important to distinguish between the expression $\phi(x)$ and the function $\lambda_x\phi(x)$ which sends x to $\phi(x)$. In particular, $\lambda_x\phi(x)`2 = 2^3 + 2 + 1 = 11$ and $\lambda_x\phi(x)`y = \phi(y) \equiv y^3 + y + 1$. In 1937, Church and Turing showed independently that every calculable numerical function can be expressed in terms of the untyped lambda calculus. In particular, the natural numbers and the usual arithmetical operations on natural numbers can be so expressed, as we shall see.

Conversely, every numerical function definable in terms of the untyped lambda calculus is calculable, thus

$$\text{recursive} = \text{calculable} = \lambda\text{-definable}.$$

According to the *Church-Turing Thesis*, any of these three equivalent concepts captures the intuitive notion of what it means to be 'computable'.

We shall now give a rigorous presentation of the *untyped lambda calculus.* We assume, to begin with, that there is a supply of countably many