Theorem 20.2. (Incompleteness Theorem)
There are mathematical formulas p such that neither p nor $\neg p$ are provable.

Proof: Let T be the set of theorems and C the set of contradictions, that is, formulas p such that $\neg p$ is a theorem. The computer can print out the members of C as easily as those of T, hence both sets are recursively enumerable. Suppose that, for every formula p, either p is provable or $\neg p$ is provable. Then p is a nontheorem if and only if $\neg p$ is provable, hence C is the complement of T. Thus both T and its complement are recursively enumerable, which contradicts the result of Church.

We should note that the incompleteness theorem was first proved by Gödel (1906–1978) and that Church used Gödel's result to prove his own. In a subsequent chapter, we shall present Gödel's original proof, which does not depend on Church's result.

21

Hilbert's Tenth Problem

Hilbert's tenth problem asked for an algorithm to determine whether any given polynomial Diophantine equation has a solution in integers. After important preliminary work by Martin Davis, Hilary Putnam (the philosopher) and Julia Robinson, Yuri Matiyasevič showed that no such algorithm exists. The proof is long and we shall give only a few of the highlights here. For a complete treatment, the reader may wish to consult Davis [1973].

First let us reduce the problem of solving a Diophantine equation in *integers* to one of solving it in *positive integers*, using the fact that every positive integer x can be written in the form

$$x = x_0^2 + x_1^2 + x_2^2 + x_3^2 + 1,$$

where the x_i are integers, in view of Lagrange's Theorem (Chapter 9). For example, if we want to know whether

$$x^{17} + y^{17} - z^{17} = 0$$

has a solution in positive integers, we may test whether the following equation has a solution in integers:

$$(x_0^2 + x_1^2 + x_2^2 + x_3^2 + 1)^{17} + (y_0^2 + \cdots + 1)^{17} - (z_0^2 + \cdots + 1)^{17} = 0.$$

A set A of positive integers is said to be *Diophantine* if there is a polynomial $p(t, x_1, \ldots, x_n)$ with integer coefficients such that $t \in A$ if and only if there are positive integers $x_1, x_2, \ldots, x_n$ such that $p(t, x_1, \ldots, x_n) = 0$. We shall write $A = A_p$ to express the relationship between the set A and

the polynomial p. For example, the set of *composite* positive integers is Diophantine of the form A_p, where

$$p(t, x_1, x_2) \equiv t - (x_1 + 1)(x_2 + 1) \equiv t - x_1x_2 - x_1 - x_2 - 1.$$

Lemma 21.1. *Every Diophantine set is recursively enumerable.*

Proof: Given the polynomial $p(t, x_1, \ldots, x_n)$ with integer coefficients and any positive integer m, let S_m be the set of all (n+1)-tuples of positive integers, each less than or equal to m. Then S_m is clearly finite. We can enumerate the elements of the Diophantine set A_p by looking at each of $S_1, S_2, \ldots$ in turn and checking whether it contains a solution of the equation $p(t, x_1, x_2, \ldots, x_n) = 0$. Whenever we do find a solution, we list its first member t.

Lemma 21.2. *Suppose there is an algorithm for deciding whether, for any given t, the polynomial equation $p(t, x_1, \ldots, x_n) = 0$ has a solution in positive integers. Then the Diophantine set A_p is recursive.*

Proof: This is so because we can perform a calculation on t to see whether $t \in A_p$.

The next lemma is due to Julia Robinson. It has to do with the notion of *exponential growth*. For example, consider the *Fibonacci sequence* F_m:

$$1, 1, 2, 3, 5, 8, 13, \ldots$$

in which each term, except $F_1 = 1$ and $F_2 = 1$, is the sum of the preceding two terms: $F_{m+2} = F_{m+1} + F_m$. This had been studied by Leonardo of Pisa (1180–1250), also known as 'Fibonacci', in connection with the growth of rabbit populations. As we saw in Part I, Chapter 23,

$$F_m = \frac{(\frac{1}{2}(1 + \sqrt{5}))^m - (\frac{1}{2}(1 - \sqrt{5}))^m}{\sqrt{5}}.$$

Since $(\frac{1}{2}(1 - \sqrt{5}))^m/\sqrt{5}$ is small, F_m is in fact equal to the integer nearest to $(\frac{1}{2}(1 + \sqrt{5}))^m$. This explains why rabbit populations grow exponentially.

Lemma 21.3. (Julia Robinson)
A sufficient condition for every recursively enumerable set to be Diophantine is that there is a polynomial equation with integer coefficients

$$p(u, v, x_2, \ldots x_n) = 0$$

such that, in its positive integer solutions, v grows exponentially relative to u.

The proof of Lemma 21.3 is too long to be included here.