Cantor’s Theorem: The power set $2^X$ of a set $X$ cannot be put into one to one correspondence with $X$. Thus the cardinality of $2^X$ is strictly greater than that of $X$.

**Proof:** Think of the elements of $X$ as some, possibly infinite, collection of people. The power set $2^X$ is the set of all subsets of $X$ and we can think of these as all possible communities made up from these people. Now imagine putting the people into one to one correspondence with these possible communities — that is, each person is assigned a unique community and vice versa. If a person is assigned to a community to which they happen to belong then call them a guard, otherwise call them a spy. The community consisting of all spies is itself a (possibly infinite) community. Is it assigned to a guard or a spy? Neither! A spy would belong to the community, so would be a guard; a guard would not belong, so would be a spy. This contradiction proves that the one to one correspondence cannot exist. QED.

This 1891 theorem about different ‘sizes’ of infinity strengthens Cantor’s 1874 Uncountability Theorem which asserts that the power set of a countably infinite set is uncountable. The above argument is essentially another manifestation of the diagonalisation method: assume some kind of listing; produce a new object for the list from existing listed objects; show that the new object invalidates the listing. The result is a well-known mathematical phenomenon: an easy proof of a deep and conceptually difficult theorem.

The notation $Y^X$ is sometimes used to denote the set of all functions mapping set $X$ to set $Y$. In the case $Y = \{0, 1\}$ this is the same as choosing subsets of $X$ (1 for include, 0 for exclude), so ‘by abuse of notation’ we write $2^X$ for the powerset of $X$. If $X$ is countably infinite, so that we may list its elements, we recover Cantor’s 1874 theorem.

**Web link:** [www.math.hawaii.edu/~dale/godel/godel.html](http://www.math.hawaii.edu/~dale/godel/godel.html)