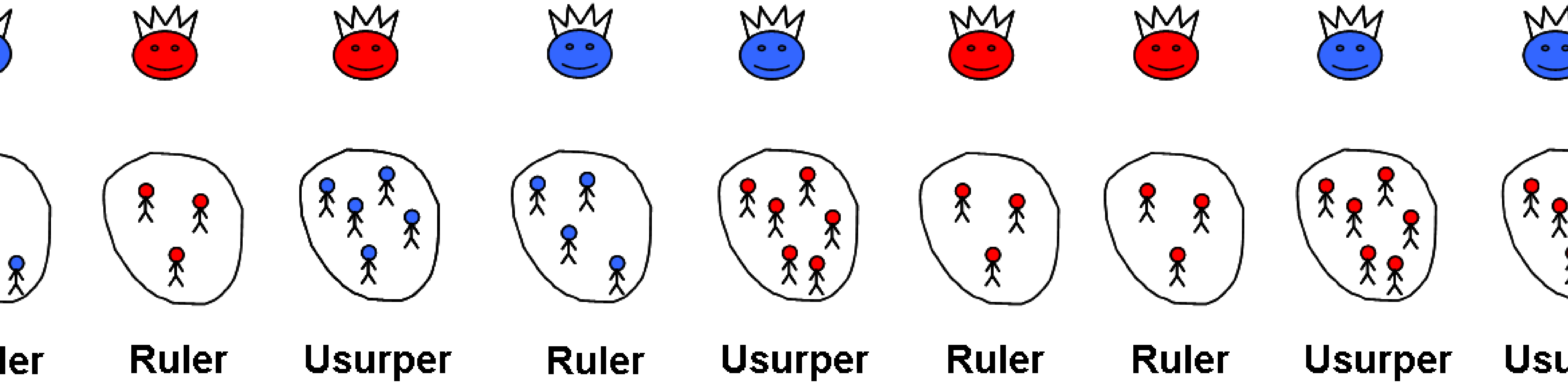
THEOREM OF THE DAY

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 *Ruler*, otherwise call them a *Usurper*. The community consisting of all Usurpers is itself a (possibly infinite) community. Is it assigned to a Ruler or a Usurper? Neither! A Usurper would belong to the community, so would be a Ruler; a Ruler would *not* belong, so would be a Usurper. This contradiction proves that the one to one correspondence cannot exist. QED.

This theorem about different 'sizes' of infinity strengthens Cantor's 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 $\mathscr{P}(X)$ is often used for power set; the notation 2^X is suggested by the fact that, for a finite set of size n, the set of all (finite) subsets has size 2^n. This follows using an 'include/exclude'-type argument that we see extended to the infinite case in the Uncountability Theorem.

Web link: www.math.hawaii.edu/~dale/godel/godel.html

Further reading: *Mathematics: the Loss of Certainty* by Morris Kline, Oxford University Press, New York, 1980.