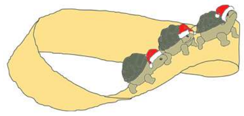

The Proof of Infinitely Many Primes

When I first presented my then hypothetical Maths Advent Calendar to my Physics teacher, his comment on my choice of topics for the articles was such that some of them were "evergreens". Were I the kind to have the occasional flutter on the horses, I would bet my money on the fact that the proof of there being infinitely many primes falls within that category. Indeed, it is an ancient concept, one going back as far as to good old Euclid, who included the proof in his *Elements*. You will have probably heard of it. If not, enjoy. It is just so remarkably cute.

Let us first recall the definition of prime numbers. Prime numbers are all those numbers which are only divisible by 1 and themselves. Euclid's theorem states that there are infinitely many of these numbers. To prove this, let us consider the finite set of primes $p_1,\ p_2, ..., p_n$ and their product $P = p_1 \cdot p_2 \cdot ... \cdot p_n$. What, we ask, are the characteristics of $P + 1$? Is $P + 1$ a prime? Is $P + 1$ a composite? Well, if the former happens to be the case, we have just managed to find a prime that was not on the list be began our multiplication with. If, instead, the latter happens to be the case, we know that none of the factors of $P + 1$ can be on our list, for each $p_1,\ p_2, ..., p_n$ divides P, and were any of them to divide $P + 1$ as well, it would also have to divide the difference between P and $P + 1$, that is to say, 1. However, no prime number divides 1, so none of $p_1,\ p_2, ..., p_n$ can divide $P + 1$ and the prime factorisation of $P + 1$ will yield prime numbers different from $p_1,\ p_2, ..., p_n$. Hence, even in this case, we have found prime numbers other than those on our list. To conclude, no matter how large a finite set of primes we manage to establish, there will always be other prime numbers that will have escaped our attention. In other words, there must be infinitely many primes!

Do you like this "evergreen"? I do.