There are INFINITELY MANY PRIME NUMBERS

$\mathscr{C} \otimes \mathscr{M} \alpha \mathscr{C}$

Some theorems, it seems, are evergreen. New proofs keep turning up for them. One such is the theorem of Pythagoras (the current number of proofs stands at over 300). Another is the claim that the square root of 2 is irrational. A third example is the statement that *there exist infinitely many prime numbers*. This is the one on which we will dwell in this short article. The proof that we feature appeared in *The American Mathematical Monthly*, in its December 2006 issue [1].

Before presenting the new proof by Filip Saidak, let us take a look at the original proof given by Euclid. We present it below. Note that it is presented in a modern form and not the form originally given by Euclid in his book *The Elements*.

Remark. In pre-algebra times, proofs were presented in a purely verbal form, using highly stylised language. Most modern readers find such proofs difficult to follow. Perhaps this is because algebra and symbolic reasoning in general have made such deep inroads into our thinking. The following example of the use of stylised language illustrates the point perfectly. It is Proposition 6 from Euclid's Elements, Book II:

> *If a straight line is bisected and a straight line is added to it in a straight line, then the rectangle contained by the whole with the added straight line and the added straight line together with the square on the half equals the square on the straight line made up of the half and the added straight line.*

Try to decipher this statement!

Keywords: Prime number, Euclid, proof by contradiction, infinite

Theorem (Euclid). ***There exist infinitely many prime numbers.***

Euclid's proof (in modern form)

To set up a contradiction, we assume that there are only finitely many prime numbers; say there are just k prime numbers where k is some finite positive integer. Let the complete collection of prime numbers be $p_1, p_2, p_3, \ldots, p_k$. Define Q to be the number obtained by adding 1 to the product of all these prime numbers. That is,

$$Q = p_1 p_2 p_3 \cdots p_k + 1. \tag{1}$$

It follows from the definition that Q leaves remainder 1 under division by each of the primes $p_1, p_2, p_3, \ldots, p_k$. That is,

$$\gcd(Q, p_1) = 1, \gcd(Q, p_2) = 1, \\ \gcd(Q, p_3) = 1, \ldots, \gcd(Q, p_k) = 1. \tag{2}$$

This implies that Q has a prime factor which is different from all the existing primes. (This prime number could be Q itself.) This is, of course, a contradiction. Hence the assumption that there are finitely many prime numbers is self-contradictory and therefore must be false. Hence there exist infinitely many prime numbers.

Proof by Filip Saidak

The new proof which we now feature shows in effect that *there can be no upper bound to the total number of prime numbers*. In short, there must exist infinitely many prime numbers. The argument is an absurdly simple one and it seems amazing that no one has found it earlier. (Perhaps this is true of any beautiful discovery.)

Here is how the argument runs. Let $N_1 > 1$ be any positive integer. Since N_1 and $N_1 + 1$ are consecutive integers, they are co-prime. This means that the set of primes that divide N_1 is disjoint from the set of primes that divide $N_1 + 1$. Hence the number N_2 defined by

$$N_2 = N_1 (N_1 + 1) \tag{3}$$

must have at least two different prime factors.

We now continue the argument with N_2 in place of N_1. Since N_2 and $N_2 + 1$ are consecutive integers, they are coprime. So the set of primes that divide N_2 is disjoint from the set of primes that divide $N_2 + 1$. Hence the number N_3 defined by

$$N_3 = N_2 (N_2 + 1) \tag{4}$$

must have at least three different prime factors.

We now continue the argument with N_3 in place of N_2 and deduce that the number $N_4 = N_3 (N_3 + 1)$ must have at least four different prime factors; and so on. It should be obvious that these steps can be continued indefinitely. It follows that the number of primes is infinite.

Closing remark.

In [1], the author notes that this proof is conceptually simpler than Euclid's original proof, as it is not based on 'proof by contradiction.' Moreover, the proof is constructive, in that it provides an explicit way of exhibiting an integer having more than any given number of different prime factors.

References

1. Filip Saidak, "A New Proof of Euclid's Theorem", *The American Mathematical Monthly* (Mathematical Association of America), Vol. 113, No. 10 (Dec., 2006), pp. 937-938. http://www.jstor.org/stable/27642094.

The COMMUNITY MATHEMATICS CENTRE (CoMaC) is an outreach arm of Rishi Valley Education Centre (AP) and Sahyadri School (KFI). It holds workshops in the teaching of mathematics and undertakes preparation of teaching materials for State Governments and NGOs. CoMaC may be contacted at shailesh.shirali@gmail.com.