Euclid, Netty, and the prime numbers

Euclid's proof that there is no largest prime has always struck me as a shining gem from antiquity; I have often used it as example when arguing that I could consider a proof a greater contribution to our culture than the theorem proved by it. I still think it a gem, but this should not close our eyes for the fact that, by now, we can do much better.

In its ugliest form, Euclid's proof is rendered along the following lines. Assume that N is the largest prime. By considering G = 1 + the product of the primes up to N, one can then establish, depending on whether G is prime or not, the existence of a prime that in either case exceeds N, thus contradicting the assumption.

Netty van Gasteren rendered Euclid's proof along the following lines. Let S be a finite set of primes. Consider G = 1 + the product of the primes in S. None of the primes in S then divides G or any of its factors. Write G as a product of 1 or more prime factors: these do not occur in S. Having thus established that no finite set S contains all primes, we conclude that the set of primes is infinite and, hence, has no largest element.

Three improvements are worth noticing:
(i) the reductio ad absurdum has been eliminated

(ii) the case analysis on whether $\mathcal{G}$ is prime or not has been eliminated
(iii) lower or upper bounds on primes have been eliminated from the argument.

* * *

None of the above is very surprising; my only reason for returning to this topic is that there is good reason to believe that by now we should be able to synthesize most of the argument. Here we go!

Our demonstrandum is "There is no largest prime number.", something we obviously cannot prove without taking some properties of prime numbers into account. What is the simplest property of prime numbers we can think of? Defining a _multiple_ to be an integer ≥2, we can state

Property 0 Each prime is a multiple.

What can we do with that in view of our demonstrandum? Well, the primes being a of integers bounded from below, we can conclude — denoting the set of prime numbers by P —

$$\text{(there is no largest prime number)} \equiv$$
$$(P \text{ is empty}) \vee (P \text{ is infinite}) \quad ,$$

and, from Property 0 all by itself, there seems litte more to be concluded. Strongly suspecting

P to differ from the empty set, we head for the new demonstrandum

"P is infite".

How does one show that a set is infite? For instance by showing that it has an infinite subset, but in a way that is begging the question, for then one has to show that that subset is infinite. I can think of only one way, viz. showing that each *finite* subset is a *true* subset. Hence our demonstrandum becomes:

"For each finite set S of prime numbers there exists a prime number that is not an element of S ."

So we have to show the existence of a prime. Do we know a property of prime numbers implying existence? Yes, we do

Property 1 Each multiple is a product of *one or more* factors, each of which belongs to P .

(In fact, it is possible to define the set of prime numbers as the *smallest* set P of multiples that satisfies Property 1. Note that we neither state nor use that each multiple has a *unique* prime factorization.)

The important thing in Property 1 is the "one or more": each multiple m leads to one or more primes that divide it. Since we are interested in the existence of a prime that does not belong to some finite S , we are interested in some multiple that no element of S divides.

Separating our concerns: for a finite set S of primes, we are looking for a $\mathcal{G}$ such that
(i) $\mathcal{G}$ is a multiple, and
(ii) no element of S divides $\mathcal{G}$.

Requirement (ii) excludes $1 \in S$, so the least we can do is to constrain S to a set of multiples. In view of Property 0 , that is a constraint we can live with. Now, a value meeting requirement (ii) is easily found —even independently of S — , viz. 1 , but, in view of (i), 1 is not a suitable candidate for $\mathcal{G}$. But our finding

$$(\underline{A}\, m : m \in S : \neg(m|1))$$

is a stepping stone since

$$(m|a) \wedge \neg(m|b) \Rightarrow \neg(m|\, a \pm b) \quad . \qquad (0)$$

Hence $(\underline{A}\, m : m \in S : m|a) \Rightarrow \neg(m|a\pm 1)$.
Since S is finite, we can choose an $a \neq 0$ so as to satisfy the antecedent, say the product of the elements in S : $(\Pi m : m \in S : m) = a$.
Since $a \geq 1$, $a+1 \geq 2$, and $\mathcal{G} = a+1$ meets both requirements (i) and (ii). Which completes the proof.

* * *

In the above, the introduction of (0) still counts as a Rabbit. Apart from that I am pleased with the synthesis of the argument. The construction of G makes quite clear

(a) that elements of S don't need to be primes and that it suffices that they are multiples

(b) that, instead of the product of the elements of S, any common multiple would have done

(c) why the 1 is added and not subtracted.

The argument also reflects nicely -as it should- that it is irrelevant that the prime numbers are smallest set P satisfying Property 1.

Austin, 19 September 1988

prof. dr. Edsger W. Dijkstra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712-1188