Primes once more (re Kac & Ulam)

The plurals are defined as the integers ≥ 2. The plurals come in two sorts, the composite numbers, i.e. the plurals divisible by a smaller plural, and the prime numbers, i.e. the plurals not divisible by a smaller plural.

Lemma 0 Each plural has a prime divisor.

Proof By mathematical induction over the plurals. Consider plural n. Either n is prime, in which case it has the prime divisor n, or it is composite, in which case it has a smaller plural divisor x which (because $x < n$) has "ex hypothese" a prime divisor that (since x divides n) is a prime divisor of n as well. (End of Proof.)

Remark The above is a nice example of what is sometimes called "course-of-values induction", in which the proof obligation is (for arbitrary n)

$$\langle \forall x : x < n : hyp.x \rangle \Rightarrow hyp.n$$

Notice in the above proof the absence of separate treatments of "base" and "step". (End of Remark.)

Lemma 1 There is no finite set of all primes.

Proof Let S be a finite set of prime numbers and consider k given by $k = 1 + \langle \Pi x: x \in S: x \rangle$ — because S is finite, the product of the numbers in S is defined —. By construction, k is not divisible by any of the primes in S — notice $\langle \forall x: x \in S: 2 \leq x \rangle$ —; by Lemma 0, however, k has a prime divisor, which therefore is a prime that is not an element of S. (End of Proof.)

(Courtesy A.J.M. van Gasteren.)

* * *

The above has been written down so that we may compare it with how Mark Kac and Stanislaw M. Ulam treat the matter on the 1st page of Chapter 1 of their "Mathematics and Logic":

> The following proof, probably still the simplest, asserts the mere existence of arbitrarily large primes. Suppose the number were finite; there would then be a largest prime p. Consider now the number $n = p! + 1$ ($p!$ is read "p factorial" and equals $1 \cdot 2 \cdot 3 \ldots p$). This number is not divisible by any prime up to p. If there is no prime between p and n, as we have assumed, then n itself would be a prime, contrary to our assumption that p is the largest one.

The authors hesitate between dealing with the number of primes and the value of primes: the first sentence deals with their values, the second one mentions

their number. The conclusion of the second sentence is unwarranted: suppose there were no primes at all, then their number would have been finite (viz. zero), but there would not have been a largest prime p. (I would like the reader to appreciate that the argument in our proof of Lemma 1 is perfectly valid when S is empty.) The second sentence would have been better, had they just written: "Suppose there were a largest prime p.".

The third sentence introduces n, the fourth sentence is the first one whose correctness depends on the concept "prime". Unfortunately, the authors opened their chapter a little bit earlier with:

1. *The Infinity of Primes*

AMONG THE SO-CALLED NATURAL NUMBERS (1, 2, 3, and so on) are some that are divisible only by 1 and by themselves; these are called the *prime numbers*. The prime numbers are the building blocks of all the numbers in the sense that every natural number is the product of powers of the primes that divide it. For instance $60 = 2^2 \cdot 3 \cdot 5$. The first several primes are 1, 2, 3, 5, 7, 11, 13, 17. It can be asked whether the series goes on forever, or, in other words, whether there is a largest prime. The answer is that there is no largest prime. This has been known since the golden age of Greece. It was proved by Euclid in the 3rd century B.C. His argument is as clear and fresh today as ever.

So, 1 is included in their primes, and the conclusion in their fourth sentence is just wrong. [This is another illustration of the fact that including 1 among the

prime numbers is an unfortunate interface.]

The fifth sentence is supposed to conclude the proof, but is very elliptic as it does not mention which property of prime numbers should justify the conclusion. It looks as if we are invited to conclude from the fact that none of the numbers between p and n is prime that none of these numbers divides n, and I hope we are not supposed to use that "every natural number is the product of [positive] powers of the primes that divide it", for otherwise we could apply the possibility of that factorization to n directly, and conclude, without the assumption that p was the largest prime, because $n \geq 2$ the existence of a prime larger than p. The last step of the quoted proof needs a possibly unstated and in any case unproven lemma (whose proof almost certainly requires mathematical induction). What an awful mess! And that in a book with the title "Mathematics and Logic"!

Now we are at it, I draw the reader's attention to the following sentence of the second quotation:

> "It can be asked whether the series [of primes] goes on forever, or, in other words, whether there is a largest prime."

However, the answer to the first question is "yes", and to the second one "no".

Mark Kac and Stanislaw M. Ulam, "Mathematics and Logic", originally published: New York: Praeger, 1968, in series: Brittanica perspective. Dover Publications, Mineola, NY, 1992

Austin, 17 March 1995

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