induction proof of fundamental theorem of arithmetic

Canonical name	InductionProofOfFundamentalTheoremOfArithmetic
Date of creation	2015-04-08 7:32:53
Last modified on	2015-04-08 7:32:53
Owner	pahio (2872)
Last modified by	pahio (2872)
Numerical id	10
Author	pahio (2872)
Entry type	Proof

We present an induction proof by Zermelo for the `http://planetmath.org/FundamentalTheore`
theorem of arithmetic.

Part 1. Every positive integer n is a product of prime numbers.

Proof. If $n = 1$, it is the empty product of primes, and if $n = 2$, it is a prime number.

Let then $n > 2$. Make the induction hypothesis that all positive integers m with $1 < m < n$ are products of prime numbers. If n is a prime number, the thing is ready. Else, n is a product of smaller numbers; these are, by the induction hypothesis, products of prime numbers. The proof is complete.

Part 2. For any positive integer n, its representation as product of prime numbers is unique up to the order of the prime factors.

Proof. The assertion is clear in the case that n is a prime number, especially when $n = 2$.

Let then $n > 2$ and suppose that the assertion is true for all positive integers less than n.

If now n is a prime, we are ready. Therefore let it be a composite number. There is a least nontrivial factor p of n. This p must be a prime. Put $n = pb$ where b is a positive integer. By the induction hypothesis, b has a unique prime factor decomposition. Thus n has a unique prime decomposition containing the prime factor p.

Now we will show that n cannot have other prime decompositions. Make the antithesis that n has a different prime decomposition; let q be the least prime factor in it. Now we have $p < q$ and $n = qc$ where $c \in \mathbb{Z}_+$ and $c < n$ with $p \nmid c$. Then

$$n_0 \;:=\; n - pc = \begin{cases} pb - pc = p(b - c) \\ qc - pc = (q - p)c \end{cases}$$

is a positive integer less than n. Since $p \mid n_0$, the induction hypothesis implies that the prime p is in the prime decomposition of $(q - p)c$ and thus also at least of $q-p$ or c. But we know that $p \nmid c$, whence $p \mid q - p$. Thus we would get $p \mid q-p+p = q$. Because both p and q are primes, it would follow that $p = q$. This contradicts the fact that $p < q$. Consequently, our antithesis is wrong. Accordingly, n has only one prime decomposition, and the induction proof is complete.

References

[1] Esa V. Vesalainen: "Zermelo ja aritmetiikan peruslause". – *Solmu* **1** (2014).

[2] Ernst Zermelo: *Elementare Betrachtungen zur Theorie der Primzahlen.* – Wissenschaftliche Gesellschaft zu Göttingen (1934). English translation in:

[3] H.-D. Ebbinghaus & A. Kanamori (eds.): *Ernst Zermelo. Collected Works. Volume I. Set Theory*, Miscellanea, Springer (2010). Ernst Zermelo: "Elementary considerations concerning the theory of prime numbers" 576–581.