Knapp, Wolfgang

On Korselt's criterion for Carmichael numbers. (English) Zbl 1370.11012

Elem. Math. 68, No. 3, 93-95 (2013).

The Korselt indicator $\kappa(n)$ for an integer $n \geq 2$ is the product of all prime numbers p for which $p-1$ divides $n-1$. The Theorem in this paper claims that the proposition

"$x^n \equiv x \pmod{m}$ for all integers x" is valid for $m = \kappa(n)$; and if it holds also for any other natural number m, then it is necessary that m be a divisor of $\kappa(n)$.

In particular, if n is a prime, then n divides $\kappa(n)$. And if n is composite, then n divides $\kappa(n)$ if and only if n is a Carmichael number, i.e., if and only if n is a product of distinct primes p for which $p-1$ divides $n-1$ – a familiar statement of the Korselt's criterion for Carmichael numbers. The known fact that Carmichael numbers are all odd follows by the observation that $\kappa(n) = 2$ if n is even, and $\kappa(n)$ is a multiple of 6 if n is odd. These corollaries, plus one more, are supposedly close consequences of the Theorem and are presented without details of proofs.

The readers should be informed that the hypothesis of the Theorem is missing the crucial assumption that $x^n \equiv x \pmod{\kappa(n)}$ for all integers x. And additionally, to be logically correct, the proof of the Theorem should replace the definition $\kappa(n) := \prod_{p \in \Phi(n)} p$ by, say, $K := \prod_{p \in \Phi(n)} p$ and show that the assumed properties of $\kappa(n)$ then force the identity $K = \kappa(n)$.

Reviewer: Amin Witno (Amman)

MSC:

11A51 Factorization; primality
11A07 Congruences; primitive roots; residue systems

Keywords:

Carmichael numbers; Korselt's criterion

Software:

ARIBAS

Full Text: DOI

References:

[1] W. ALFORD, A. GRANVILLE, C. POMERANCE: There are infinitely many Carmichael numbers, Ann. of Math. 139, 703-722 (1994). · Zbl 0816.11005 · doi:10.2307/2118576

[2] R. CANDALL, C. POMERANCE: Prime Numbers, a computational perspective. Springer Verlag 2001.

[3] R.D. CARMICHAEL: On composite numbers P which satisfy the Fermat congruence a P - 1 \equiv 1 (mod P), American Mathematical Monthly 19 (2) 22-27 (1912). · Zbl 42.0236.07

[4] O. FORSTER: Algorithmische Zahlentheorie, Verlag Vieweg 1996.

[5] A. KORSELT: Probl'eme Chinois, L'intermédiaire des mathématiciens 6, 142-143 (1899).

[6] P. RIBENBOIM: The New Book of Prime Number Records, Springer Verlag 1988-1996. · Zbl 0642.10001

[7] H. SCHEID, A. FROMMER: Zahlentheorie, Spektrum Akademischer Verlag 2007.